Code of Conduct on the use of GDPR compliant pseudonymisation

Preface

The pseudonymisation of personal data is becoming an increasingly important topic, especially in light of the role digital platforms and the platform economy play in our society. Platforms possess enormous amounts of data that are often used for the purpose of profiling users, or for the development and implementation of AI applications. By using the technique of pseudonymisation, a functional contribution can be made to ensuring that the personal rights of users are protected when operating digital platforms, such as with regard to individualised profiling. Pseudonymisation can also play a pivotal role concerning other scenarios for processing of personal data where safeguards for data subjects are deemed necessary.

Art. 4 (5) of Regulation (EU) 2016/679 (GDPR) 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". Moreover, such additional information is meant to be kept separately and must be subjected to technical and organisational measures that ensure that the personal data are not unduly attributed to an identified or identifiable natural person.

As stated by the GDPR itself, "[a]ssociations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation" (Art. 40 para. 2). Codes are thus meant to specify and concretise the abstract principles of the GDPR. As stated by the Regulation itself "the pseudonymisation of personal data" is one such facet of the Regulation whose application can merit from further specification.

The purpose of this voluntary 'Code of Conduct on the use of GDPR Compliant pseudonymisation' ("Code") is thus to further specify the application of pseudonymisation as it is used throughout the GDPR, in particular in Art. 4 (5); Art. 6 para. 4 (e); Art. 25 para. 1; Art. 32 para. 1 (a); and Art. 89 para 1. The development of this Code gives controllers and processors the opportunity to carry out pseudonymisation based on transparent guidelines, which in turn reduces legal uncertainty and allows them to streamline their technical processes. Data subjects benefit from the application of uniform standards, allowing an increase of trust in data driven system and applications. The Code has thus been prepared to contribute to the proper application of the GDPR, taking into account the specific circumstances of the pseudonymisation process.

Since the Code has a transnational character (i.e. ,it relates to processing activities in several Member States) it must be submitted to the competent national supervisory authority which initiates the consistency mechanism referred to in Art. 63. .

Codes of conduct are expected to be continuously updated and developed. The same applies to this Code. At a minimum, future updates are expected regarding Good Practices and further transition and elaboration of sub-sector specific guidance. In other words, the existing application examples will be expanded to include sub-sector-specific Good Practices in chapter 5 so the roadmap offered by this Code is supplemented by real-life examples of how specific problems are dealt with on a case-by-case basis. This will not only help other organisations to find appropriate solutions to new, unforeseen situations, but it can also help data subjects by demonstrating precedents in the effects of specific cases and offering a transparent look into the controller's or processor's problem-solving.

Content

1 Introduction

The aim of this Code is to specify the application of the GDPR regarding pseudonymisation, as suggested by Art. 40 para. 2 (d) GDPR. Pseudonymisation protects data subjects from unwanted identification and is an implementation of the principle of data minimisation found in Art. 5 para. 1 (b) GDPR. It constitutes a technical and organisational protection measure in accordance with Arts. 25 and 32 GDPR. It can also influence the lawfulness of the processing of personal data, as Art. 6 para. 4 (e) GDPR determines.

It thus fulfils both a protective and an enabling function. According to its definition in the GDPR, pseudonymisation is characterised by the fact that personal data are processed in such a way that these data can no longer be attributed to a specific person without additional information (cf. Art. 4 para. 7 GDPR).

Even though the identification of an individual is possible within the scope of a pseudonymisation, this must be prevented by means of technical or organisational measures apart from a desired disclosure. The GDPR does not contain any detailed provisions on how pseudonymised data can be created by technical or organisational measures, nor on possible protective measures regarding the pseudonymised data.

Therefore, this Code defines both procedural as well as organisational and technical requirements, which enable both controllers and processors to implement the pseudonymisation in a practical way.

2 Scope of application

As stated in para. 23 of the EDPB's 'Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679', a draft code "must have a defined scope that clearly and precisely determines (…) the categories of controllers or processors it governs".

This Code applies to controllers and processors, regardless of their industry or sector, if they pseudonymise personal data themselves in accordance with the requirements of the GDPR or if they are responsible for the pseudonymisation process. This broad understanding of a sector is supported by the EDPB's Guidelines on Codes of Conduct as a tool for transfers[1].

The Code's statements apply independently of the internal organisational responsibilities and distribution of tasks among controllers or processors.

Controllers or processors who use pseudonymised data in their services or products, thus are managing a pseudonymisation process, may join this Code to prove that the pseudonymised data was created in accordance with the rules defined herein. They can decide for themselves which pseudonymisation processes are to be subjected to this Code. In the case of those products, services or other data processing that fall back on pseudonyms that originate from pseudonymisation processes that were subject to this Code, this must be pointed out transparently.

[1] EDPB Guidelines 04/2021, para. 6, in their version of July 7th, 2021.

3 Definitions

Where this Code uses the terms defined in the GDPR, those terms shall have the same meaning as in that Regulation unless explicitly stated otherwise.

For the purposes of this Code:

- **Pseudonymisation** means pseudonymisation in the sense of Art. 4 (5) GDPR: 'pseudonymisation' [means] 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. According to Art. 4 (5) GDPR, the additional information is the only information with which the connection of a pseudonym to the person represented can be established. Depending on the pseudonymisation method, the additional information can be a direct assignment or an assignment rule.

- A **pseudonym** is an attribute, like a string of characters, that replaces data directly identifying an individual data subject and thus indirectly represents that data subject.

- The **pseudonymisation method** or **procedure** describes the technical-organisational process which ensures that personal data can no longer be attributed directly to an identified or identifiable natural person.

- **Specialist managers** are all persons or departments within a company who are not responsible for the organisation of all processing activities, but who design individual sub-areas in compliance with data protection regulations (such as the proper pseudonymisation of personal data).

- The **Specialist Responsible for Pseudonymisation (SRP)** are all persons or departments within a company who are responsible for the design of the pseudonymisation process in accordance with data protection regulations, at least in the form of a supervisory and advisory function.

- An **incident response** plan is a set of instructions to help controllers and processors to detect, respond to, and recover from a personal data breach.

- **Anonymous information** is information which does not relate to an identified or identifiable natural person.

- **Allocation table** is a list that compares identity data and pseudonyms. Such list can be used to determine a person's pseudonyms directly from the individual's identity data and vice versa to determine an individual's identity data from a person's pseudonym.

- A **homonym error** occurs if identity data of different persons falsely lead to the same pseudonyms.

- A **cryptographic hash function** is a function that assigns a string of any length to a string of fixed length (e.g. 256 bits). A cryptographic hash function also has the property of a one-way function. If, in addition, it is practically impossible to find two different input values that provide the same function value, one speaks of a collision-resistant hash function. Internationally standardized cryptographic hash functions are MD5, SHA256 or SHA-3.

- **Block cipher** is an encryption method which transforms a data block of fixed length (e.g., 128 bits) into a block of the same length depending on a cryptographic key. The most common block encryption method today is the AES (Advanced Encryption Standard), which encrypts 128-bit blocks using a 128-,192- bit or 256-bit key.

- **Entropy** is a measure of the indeterminacy of a sequence. For example, ten independent coin tosses (head/number) provide ten bits of entropy. If a sequence is calculated from an initial value ("seed") using a pseudorandom number generator, it can never reach a higher entropy than the initial value.

- **Signatory** means any entity that successfully declared one or more PP adherent to the Code.

- A **salt** is comprised of randomised data used as an additional input such as when using one-way functions.

4 Process specifications for the use and operation of pseudonymisation

4.1 Organisational questions

4.1.1 Designate the person responsible for the entire process

From an organisational point of view, the controller or the processor shall appoint a Specialist Responsible for Pseudonymisation (SRP). The overall responsibilities and duties of the controller laid down in the GDPR are not transferred. This SRP shall coordinate the individual organisational responsibilities before, during and after the pseudonymisation process.

> *Explanation: Here, the term SRP does not mean the controller in the sense of the GDPR, but the person internally responsible for the organisation and the proper process of pseudonymisation. The pseudonymisation of personal data is usually part of a more general processing activity (according to the record of processing activities).*

The SRP can also take on other specialist responsibilities or take overall responsibility for the respective data processing. In any case, the responsibility of this person or department shall be documented as SRP regardless of other responsibilities. The appointment of a data protection officer as SRP is not permitted.

The SRP shall possess the technical and organisational expertise required for pseudonymisation. If a department has been designated as SRP, the department shall have the necessary specialist knowledge if and to the extent that it is ensured from an organisational point of view that this department always exercises its responsibilities. It shall suffice that required specialist knowledge is held by multitude of a department's personnel; explicitly it shall not be required that each personnel of such department hold all relevant applicable specialist knowledge individually.

> *Explanation: The SRP is not to be equated with the data protection officer of the controller or processor. In contrast to the SRP, the data protection officer is not responsible for the lawfulness of data processing. His/her legal duties are defined in Art. 39 GDPR and are characterised by giving advice and to monitor. In the area of pseudonymisation, the data protection officer can advise on the planning and implementation of the pseudonymisation, as well as monitor compliance with the legal requirements for pseudonymisation and this Code. Due to the allocation of organisational responsibility to the SRP, the data protection officer and the SRP cannot be identical as this would not be compatible with the legal requirements.*
>
> *To the extent specialist managers or specialist departments are being implemented, appointed departments and individuals already presuppose comprehensive data protection expertise. Such expertise should be enriched, if necessary, by those aspects that are required for the support and implementation of pseudonymisation, e.g., by integrating relevant aspects into existing training and continuing education measures. In addition to such training measures that take place anyway, special expertise can also be made available through recourse to a central data protection department or, in particularly complex and differentiated structures, a central department for pseudonymisation. In this way, such a central department can already work out predefined processes which the SRP is obliged to adhere to. In this case, such a process can (and should) also regulate significantly more precise obligations than this Code. For example, considerations could already be made as to which types of data may only be fed to certain pseudonymisation processes, or which specific precautions are to be taken in the event of re-identifications that are to be expected on a regular basis.*

It is also possible to specify how and where certain documentation is to be carried out, for example, to ensure technically supported compliance. Such a technically supported system also makes it easier to find existing documentation and information and to reuse it in the context of the specific pseudonymisation decision. The consistency achieved in this way minimizes conflicts in the processes and thus also facilitates their (internal) verifiability.

Specialised and centralised departments may also beneficially support the implementation of pseudonymisation in a twofold manner: On the one hand, the specialist department or the individual designated for this specialist department is the first point of contact for other departments – such as Group Privacy and / or Compliance. On the other hand, units downstream of the specialist departments can contact the specialist department in the event of queries. The defined responsibility also helps to ensure that there is a central overview of the pseudonymisation to be performed, which. in particular. makes it possible to verify that the considerations and process steps for pseudonymisation have been documented.

4.1.2 Assessment and documentation of the criteria necessary to determine the pseudonymisation method

For the legally compliant use of pseudonymisation, the following criteria shall be considered in documented form.

4.1.2.1 Type and risk class of personal data processed

The type and risk class of the data processed shall be specified to ensure pseudonymisation in conformity with data protection regulations. The selection of the adequate, GDPR compliant pseudonymisation procedure must take place based on this risk assessment.

Explanation: In principle, there can be different categories of data:

- *Personal data pursuant to Art. 4 (1) GDPR*
- *Special categories of personal data pursuant to Art. 9 (1) GDPR*

The categories of data processed can be found in the record of processing activities.

Within the framework of the risk assessment of the processed data, assessments from risk analyses or a data protection impact assessment can also be applied.

The data category used does not represent a suitable criterion for a risk assessment in itself and can at best be used as an indication. Rather, other aspects must also be considered within the framework of a risk assessment. This included, for example,

- *the purpose and context of the processing (see below 2.1.2.2. and 2.1.2.3.); for example, identical personal data may be used in the context of contract performance or to track user activities;*
- *the category of data subjects; e.g. children or members of certain population groups without immediately triggering the scope of application of Art. 9 (1) GDPR;*
- *the number of persons concerned (see 2.1.2.4 below) or the combination of the different data categories.*

4.1.2.2 Intended processing purposes

The purposes for which the data are to be processed shall be specified. They shall be sufficiently precise to allow the purpose limitation principle to be respected.

Explanation: There may be more than one purpose of processing. Purposes cannot easily be changed in the aftermath of data collection, so that these should be documented as comprehensively as possible. Examples for a processing purpose may include data processing for billing purposes, for checking the network utilisation of a mobile phone provider, for product development purposes or for the

processing of data for research purposes. Research purposes should be specified in the documentation to the extent that the research context or the research objective can actually be comprehended in terms of whether an actual, future processing is subject to the intended research purpose and therefore a risk assessment can also be adequately derived. The description of the purpose also has an influence on the assessment under data protection law as to whether data processing for the intended purposes still falls within the scope of the relevant statutory provision and, on the other hand, such description enables organisations to examine whether pseudonymisation changes this assessment in some way.

4.1.2.3 Context of pseudonymisation

The context of pseudonymisation shall be documented.

Explanation: The context of processing refers to the legal context for pseudonymisation. Pseudonymisation can be used, for example, in the course of its enabling function within the framework of Art. 6(1)(f) and Art. 6(4) GDPR or as purely technical and organisational measures pursuant to Art. 32 GDPR or within the framework of Art. 25 GDPR. The context and purpose of pseudonymisation are usually defined by the departments. Documentation is necessary because this context also influences the choice of the appropriate pseudonymisation procedure.

4.1.2.4 Expected number of processed records

It shall be checked and documented how many records will be processed.

Explanation: From a technical and organisational point of view It makes a difference whether only a few data sets or a large number of data are pseudonymised. When checking the number of data records to be processed, it is relevant whether the data records are static or dynamic, i.e. whether they are a fixed number of data that is pseudonymised or whether the data record is continuously enriched with further data. Classical list procedures for pseudonymisation using tables are for example not suitable for a large amount of data.

4.1.2.5 Suitable pseudonymisation types

The different types of pseudonyms required for the intended processing purposes and context shall be documented.

Explanation: Different types of pseudonyms are particularly suitable for certain purposes, although they may be completely unsuitable for other purposes.

A distinction can be made between the following types of pseudonyms:

- *Personal pseudonyms that replace identity data such as name, ID number or mobile phone number*
- *Role pseudonyms where one or more persons are assigned to a pseudonym (e.g. IP number)*
- *Relationship pseudonyms where a person uses a different pseudonym for each (communication) relationship, e.g. different nicknames, role relationship*
- *Role-relationship pseudonyms that are a combination of the two pseudonym types*
- *Changing pseudonyms where, for example, a new pseudonym is used for each transaction or each entry. Used, for example, in online banking*

Considering the purpose and context of the processing, those types of pseudonyms shall be preferred which are suitable for the respective purpose and at the same time protect the data subject as far as possible against unwanted re-identification. The SRP shall support regarding the selection of the appropriate type of pseudonymisation. The weighing carried out for the decision for or against a relevant type of pseudonymisation must be documented.

Explanation: In general, the risk of reversal of personal pseudonyms is higher than that of role or relationship pseudonyms. This is related to the persistent connection of a pseudonym with the individual person. Depending on the purpose and context of the processing, the use of personal pseudonyms may be necessary. On the other hand, there is a lower risk of reversal of persons with role-relationship pseudonyms and changing pseudonyms than with the abovementioned person pseudonyms.

4.1.2.6 Determination of the appropriate pseudonymisation method and the time of pseudonymisation

Different methods are available for pseudonymisation.[2]

The strength of the applied method shall be examined, determined, and documented considering all objective factors, risks to the rights and freedoms of the parties concerned as well as the costs of re-identification and the time required for this when using the technologies available at the time of processing as well as foreseeable technological developments. When using calculation methods, a state-of-the-art transformation procedure shall be used (for technical requirements, see 2.2.1.).

Pseudonymisation procedures shall be designed in such a way that simple and efficient selection and deletion of the data is possible, insofar as the processing purpose no longer exists or the legal basis for the processing is no longer applicable.

Such pseudonymisation methods shall be preferred which enable the subsequent anonymisation of data.

The pseudonymisation shall be applied to in the processing process as early as possible.

Explanation: The principle of data minimisation and the principle of privacy by design are stipulated in the GDPR (Art. 5(1)(c), Art. 25). As a result, the technical design can provide the appropriate framework conditions from the beginning. Compliance with these principles avoids the per se inadmissible unlimited retention of pseudonymised data.

If the pseudonymisation has been identified as suitable processing by the controller or processor, the Code requires its technical implementation to be carried out promptly to comply with the data minimisation principle. Likewise, controllers and processors need to ensure that pseudonymisation is carried out as early as possible in multi-stage data processing, especially if non-pseudonymised data are not required at the upstream processing stages.

4.1.2.7 Planned disclosure of pseudonymised data

It shall be documented whether pseudonymised data are to be transmitted to third parties. Such documentation shall include information on how that third party has been duly selected.

The data controller or processor shall take appropriate measures to ensure that the pseudonymised data is only processed by the recipient(s) for the purposes specified beforehand.

The controller or processor shall ensure that the transfer of the pseudonymised data to the recipient is covered by a legal basis.

The data provider as well as the recipient shall agree on a purpose for processing before pseudonymised data is transferred. Such agreement shall be confirmed by the recipient.

The controller or processor shall take appropriate measures to prevent the recipient from inadmissibly re-identifying data subjects. No additional information shall be transmitted that could lead to the identity of a data subject being inferred.

---

[2] European Union Agency for Cybersecurity, Pseudonymisation techniques and best practices (November 2019), https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

Explanation: The evaluation of the pseudonymised data usually requires special knowledge that may not be available in the actual specialist department. It may also happen, that for product improvement and enhancement, services of an external service provider will be used. This usually comes along with pseudonymous data being stored by this external service provider. To keep an overview of third parties storing pseudonymised data, the Code stipulates documentation obligations. According to the Code, these third parties may also be other departments and companies of the same enterprise. The documentation can take place within existing frameworks, such as of the directory of processing activities.

The GDPR applies to the processing of pseudonymised data, including the purpose limitation pursuant to Art. 5(1)(b).

The purpose of the processing can be confirmed by the recipient in text form or in writing (e.g. as part of a contract) as an appropriate measure. Since the transfer of pseudonymised data falls within the scope of this Code, a possible re-identification of data subjects within the scope of the data transfer has to be taken into account. The Code therefore formulates an obligation for the data provider to take appropriate measures in this regard before passing on the data to the recipient. This includes, for example, an obligation to check on the part of the recipient regarding obvious identification possibilities. The data providers detailed knowledge of the possibilities of linking the data on the recipient´s side though cannot be assumed. In any case, a supplementary confirmation by the recipient can be obtained by the data provider in text form or in writing (e.g. as part of a contract) that a re- identification does not take place by the recipient. Since the transmission only serves the purpose of evaluating the information for the transmitting body in a value-added manner, other processing can be explicitly prohibited.

Insofar as an audit has shown that the recipient could obviously carry out a re-identification, appropriate supplementary protective measures need to be implemented as far as this appears necessary due to the expected risks for the data subjects.

4.1.2.8 Planned processing of pseudonymised data in the third country

It shall be documented whether pseudonymised data are to be processed outside the EEA. In the event of the transfer of personal data to a third country, the data controller or processor shall ensure that the requirements of Chapter V of the GDPR are met. When collecting personal data, the data subject shall be made aware of the transfer of such data to a third country, even if pseudonymised data are transferred.

Explanation: The GDPR places special requirements on the processing of personal data in a third country outside the EU or the EEA. These requirements are regulated in Chapter V of the GDPR and include, for example, the transfer of personal data based on an adequacy decision by the EU Commission or other suitable guarantees according to Art. 46 GDPR. The fact that the data to be transferred are pseudonymised do not exempt the data exporting body from complying with the requirements of Chapter V. After all, a data subject can also be re-identified in a third country using the key to pseudonymisation.

4.1.2.9 Planned/ foreseeable frequency of re-identification

The planned or foreseeable frequency of re-identification of data subjects shall be specified in documented form.

The planned or expected reasons or for which purposes re-identification will take place shall be documented. (e.g. to safeguard the rights of the data subjects).

In addition to the reasons and purposes, it shall be documented what delay of tolerance exists in the event of re-identification, i.e. what the maximum delay may be until sufficient re-identification of a data set.

Explanation: The chosen processing purposes have an influence on the question of whether a re-identification of the data subjects will be carried out promptly and in the short term. In the area of network monitoring, for example, it may be necessary to identify a workstation infected with malicious code based on pseudonyms at short notice. Therefore, the Code requires controllers or processors to define the planned or expected frequency of re-identification of data subjects,

Pseudonymisation methods differ, among other things, in their efficiency and manageability regarding the re-identifications that have to be carried out. Similarly, the frequency of expected re-identifications also interacts with an appropriate allocation of functions as defined in Section 2.1.3. The documentation to be prepared here should enable the SRP to create a binding basis for consideration. On the other hand, it should enable the SRP to evaluate the hypothesis and planning presented here over time. Such an evaluation would have to consider, for example, whether a possibly very high, expected re-identification rate actually occurs in practice. It would also be necessary to consider, for example, whether the delay tolerance could be adhered to or whether other pseudonymisation methods are now also able to adhere to these tolerances due to new technical developments.

4.1.3 Risk-adequate concept for rights and roles

Regarding access to pseudonymised data and the combinations thereof required for the respective activity, possible existing translation tables and keys for the re-identification of the data subject and other information, an appropriate rights and role concept based on the need-to-know principle shall be provided and documented. The more sensitive the processed data or the higher the expected risks for the rights and freedoms of the data subjects, the more effective such access controls shall be.

Explanation: According to the legal definition of pseudonymisation, additional information that enables the re-identification of data subjects must be kept separately and identification must be prevented by technical and organisational measures. An existing rights and role concept can represent such a technical-organisational measure. If the existing rights and roles concept does not sufficiently address the specific requirements in individual cases, this would either have to be adapted or supplemented by a specific concept. Depending on the risk of the data and the context of the processing, different models are suitable within such a rights and roles concept:

"All-in-one-hand"-model: Here, the controller or processor has both the pseudonymised data and the possibility at any time to reverse the processed pseudonyms or to re-identify the data subject. A possibility of re-identification can be assigned to a person, a department, or a legal entity. Also, the definition of internal requirements, which would result in permissible and impermissible circumstances for carrying out a re-identification as well as possible documentation obligations regarding re-identifications are considered suitable technical and organisational measures.

Trustee model: In the classic trustee model, the trustee is a legal entity outside the controller or processor acting as a "third party". It is therefore a trust centre that is independent of data collection and usage in terms of location and organisation. A trustee can, for example, be entrusted with the storage of keys for the re-identification of data subjects. The processing of pseudonyms by the third party is also a possibility, while any keys and raw data remain with the controller or processor.

Key management is the most common scenario in which a trustee can be involved in various ways. The method chosen within the trustee model should be based on the documented risks for the data subjects. Examples are

- *Ex ante: The trustee re-identifies the data subjects for purposes or circumstances defined prior to the commencement of processing.*
- *Ad hoc: The trustee re-identifies the data subjects based on previously defined consideration criteria, but not according to previously defined purposes and circumstances.*
- *Ex post: The trustee is informed of any re-identifications that have taken place, together with the reason (e.g. as an individual case or via statistics). The trustee can evaluate this information and take appropriate measures based on it, e.g. training or disciplinary measures.*

Mixed models: Mixed models are also conceivable. Here, for example, the separation of the information necessary for re-identification can also take place within the organisation of the controller or processor, in which the information is subjected to a rights and role concept. This can also include, for example, distributing information across several hierarchical levels or independent departments. The departments usually responsible for such issues (internal audit or compliance or legal department, (IT) security or data protection officer) could also be suitable for this purpose anyway. Particularly in large organisations, the establishment of a trustworthy "third party" of its own, which offers the separate administration of data and/or secrets or keys internally, is also an option.

Such mixed models are conceivable, for example, particularly in cases where the processing comprises several processing steps and several pseudonymisation stages, for each of which different risks to the data subjects have been determined.

4.1.4 Definition of guidelines for re-identification

If a re-identification of data subjects on the basis of the pseudonymised data is envisaged, the following requirements shall be observed and documented:

1. In the case of pseudonymisation as a protective measure according to Art. 32 GDPR, no permission to trace pseudonyms back to individuals is required beyond the original legitimation for data processing. The reversal is covered by the original purpose of use.

2. In the case of pseudonymisation to enable the further processing of data in accordance with Art. 6 para. 4 GDPR, the following applies:

   - In cases where the data subject has an overriding interest in being re-identified (e.g. for the purpose of information or an opportunity to object), the admissibility must be examined in relation to the data processed (Art. 6 or Art. 9 GDPR).

   - In cases where it cannot be established whether the data subject has an interest in being re-identified, consent to re-identification must be obtained. This does not apply to re-identification based on a legal permission or obligations.

   - In cases where the controller has an overriding interest concerning re-identification of the data subject (e.g. for the purpose of providing information), the admissibility of re-identification must be individually assessed (Art. 6 para. 4 GDPR)

3. In cases where a dynamic data set (cf. 2.1.2.4) is pseudonymised, it must be checked at regular intervals whether this dynamic data makes it possible to re-identify data subjects. In the event of the possibility of re-identification, the provisions of paragraphs 1 and 2 shall apply.

4. The SRP shall advise the controller or processor during this assessment.

4.1.5 Unintentional/unlawful reversal of a pseudonymisation

In the event of an unintentional or unlawful reversal of a pseudonymisation, an incident response plan must be drawn up. The SRP shall support this procedure. The response plan, which has to be documented, shall include the following elements:

- Risk assessment for data subjects

- Measures to prevent/control the risk

- Evaluation of a notification obligation according to Art. 33/Art. 34 GDPR (as controller or processor)

- In case of acting as controller: Notification to the supervisory authority and the data subjects in case of the existence of an obligation to notify.

The incident response plan can be integrated into an existing process (for example, Data Breach Incident Response Plan) at the controller or processor.

Explanation: According to Recital 85 sentence 1, the reversal of a pseudonymisation can constitute a data breach which, in the event of a risk associated with the breach for the data subjects concerned, must be reported to a supervisory authority or, in the event of a probable high risk, also to

the data subjects. To comply with Art. 33/Art. 34 GDPR, controllers and processors must take any necessary steps into account in a response plan in the event that a pseudonymisation is reversed. The incident response plan does not have to be created separately for the pseudonymisation but can generally exist for data protection incidents at the controller or processor, but must explicitly address the reversal of a pseudonymisation.

4.1.6 Definition of a regular review process concerning the necessity of processing

The intervals shall be defined and documented at which the necessity of processing of pseudonymised data has to be assessed. The SRP provides advice and support in this regard. Such a review shall take place at least every two years. The assessment shall be documented. If, in the course of this review, it is determined that processing is no longer necessary, the pseudonymised data shall be deleted or be rendered to anonymous information in accordance with data protection regulations.

Explanation: Since pseudonymised data make it possible to re-identify data subjects, such processing activity is also subject to the principle of storage limitation under Art. 5 para. 1 lit. e GDPR. If pseudonymised data are no longer required for the specified purpose of processing, they must be deleted. Consequently, it is necessary to establish a regular cycle for an assessment of necessity by the controller or processor to determine the necessity of the processing.

4.1.7 Notification obligations to supervisory authorities in special cases

If, despite pseudonymisation will be applied as an isolated measure or amongst other measures, and, following a Data Protection Impact Assessment (Art. 35 GDPR), a high risk for rights and freedoms of data subjects can still be identified within the scope of a processing activity, the competent supervisory authority pursuant to Art. 36 GDPR shall be consulted. The SRP shall be involved in such consultation.

Explanation: Controllers must consult the supervisory authority in advance of any processing if a data protection impact assessment pursuant to Art. 35 GDPR has been conducted, but the processing still would pose a high risk to data subjects, unless additional measures are taken to contain such risk. If there is a high risk for data subjects and pseudonymisation is the only protective measure, there is a legal obligation to consult the competent supervisory authority.

4.1.8 Documentation and regular evaluation of the process, the considerations made, and the measures actually taken

For each section of Section 4.1, the measures taken as well as the influencing factors for determining an appropriate pseudonymisation method (Section 4.1.2) shall be documented.

Insofar as the determination of the measures taken is to be preceded by an assessment, such assessments shall also be documented. The assessment shall be prepared by the SRP. It shall be ensured that modifications of the documentation are exclusively transparent; in particular regarding the aspects "what", "by whom" and "when".

Explanation: From an accountability perspective it is important that the decision-making of a suitable pseudonymisation method is transparent. Documentation plays a pivotal role here. The SRP can fall back on documentation from other technical experts and third parties when preparing the documentation.

4.1.8.1 Documentation of processes and other measures taken

Processes and measures taken shall be documented in such a way that

1. the SRP is capable

- to evaluate the process or measure in terms of effectiveness;

- to verify the implementation of the processes or the measures taken;
- to evaluate compliance with the processes or measures taken, as well as,

2. the SRP and all persons entrusted with implementation are able to

- understand the process or the measure and to implement it according to the defined specifications.

> *Explanation: Irrespective of individual, supplementary documentation, documentation may regularly be provided in the records of processing activities or any other already existing frameworks. In complex structures in particular, systems may become handy in which the records of processing activities does not contain the information directly but refers to relevant and pertinent documents elsewhere in a sufficiently precise and comprehensible manner. Such an approach may support any central processes to be implemented uniformly.*

4.1.8.2 Documentation of considerations

Considerations shall be documented, including a statement of reasons. It shall be ensured that the conclusions reached within the framework of the consideration – e.g., determination of the appropriate pseudonymisation method or an applied risk classification – can also be easily understood by third parties. These considerations shall be reviewed regularly, in particular regarding the state of the art and conformity with the intended purpose, and these reviews shall also be documented. References to already existing documentation shall be permissible. The reference shall entail the concrete title, storage or storage location and version of the referenced document.

> *Explanation: The documentation to be prepared in accordance with this section fulfils several objectives. The documentation forces the controller or processor to systematically process the requirements of this Code. Insofar as the SRP makes use of the services of other specialist managers, the SRP shall have an information base which is always comprehensible also for him/herself. This documentation also enables the SRP to review the original assumptions regularly and adjust them if necessary. Such an evaluation is necessary to the extent that the GDPR requires processing in accordance with the current state of technology. It is therefore likely that measures taken, or considerations made based on documented information will have to be modified as the technical status quo progresses. The documentation also enables both the SRP and any compliance departments to carry out conformity checks.*

4.2 Technical questions

4.2.1 General requirements for pseudonymisation

The technical implementation shall take place only in consultation with the SRP. The SRP shall consult the specialist managers when selecting and evaluating the appropriate pseudonymisation method. The specialist managers shall also consult the SRP on intended changes to the technical implementation.

> *For the implementation of a pseudonymisation, different procedures can be used. For example, an allocation table can be used in which one or more pseudonyms are allocated to each date in plain text. Alternatively, various cryptographic methods can be used for pseudonymisation, each of which converts a plain text date into one or more pseudonyms. The reversibility of pseudonymisation can be controlled/restricted here by establishing access controls concerning used cryptographic keys and, if necessary, other parameters.*

When selecting the pseudonymisation to be used, the initial assessment steps (in particular, subsections 4.1.2.1to 4.1.2.6) shall be followed.

4.2.2 General requirements for Identifiers (IDs)

Regardless of the other requirements, an ID shall be used as a pseudonym that does not allow any conclusions to be drawn about the input data or the natural person concerned.

Application scenarios and challenges:

1. When pseudonymising data, it shall be ensured that the ID used cannot be re-identified if individual information in the data set is viewed in context with other data.

   Explanation: The postal code is used as the ID; the data also contains individual information about the date of birth. With a sufficiently small number of data sets, the natural person can be re-identified by comparing all data sets with identical birth data.

2. If IDs are generated based on the combination of individual information in the data records under consideration, it shall be ensured that a direct comparison of the output data with the input data or knowledge of the applied scheme does not allow for effortless re-identification, for example, by adding a secret key ("salt") to the process of generating a pseudonyms.

3. Preference shall be given to methods which do not allow any conclusions to be drawn about the sorting of the data, neither before nor after any pseudonymisation method will be applied; sorting shall be sufficiently random.

   Explanation: Pseudonymised data could be re-identified by an easily understandable chronological or alphabetical sequence.

Regarding the technical procedures applied, relevant current technical guidelines shall be considered. Transformation procedures used for pseudonymisation shall be replaced by state-of-the-art procedures where necessary– to guarantee a maximum of security. This shall consider, besides others, the period for which the pseudonyms will be used.

Explanation: A reasonable starting point for current technical guidelines may be those by BSI[3] and ENISA[4].

4.2.3 Calculation method

The choice of the specific pseudonymisation method shall be based on the initial assessment (Section 4.1.2.1 until 4.1.2.6) and coordinated with the SRP; accordingly, the technical implementation shall be subject to regular evaluation, cf. 4.1.8.2.
When using calculation methods to determine pseudonyms (in particular for pseudonymous users), it shall be ensured that these have the following properties:

1. They must be based on state-of-the-art secure cryptographic methods.

   Explanation: Software to create pseudonyms should use available crypto libraries instead of re-implementing the algorithms. This is why Open-Source implementations are useful.

2. For the given plain text space (e.g. the set of all user IDs or names or telephone numbers) the function pseudonym = f (plaintext ID) must be unique, i.e. different pseudonyms must result for different plain text keys in order to avoid homonym errors.

   Explanation: A homonym error occurs if identity data of different persons falsely lead to the same pseudonyms.

3. The inverse function plaintext ID = g (pseudonym) must not be calculable with reasonable effort.

[3] To be added

[4] To be added

Explanation: The reasonable effort should also be determined based on the specific circumstances. In particular, the value of the re-identified data for unauthorised parties should be considered. The risk analysis carried out can be used for this purpose. This information is important for the determination of the reasonable effort, as it allows conclusions to be drawn about the expected technical and professional resources of unauthorised parties: The higher the value of the data, the greater the effort that can be expected from the point of view of unauthorised parties.

4. Similar, especially consecutive plaintext IDs must not lead to similar pseudonyms, small changes to plaintext IDs must lead to completely different pseudonyms to make it more difficult to "guess" plaintext IDs.

5. The security of pseudonymisation must not be achieved by keeping the algorithm secret, but by using a secret key.

6. From the knowledge of a pair (plaintext ID/pseudonym) it must not be possible to deduce the secret with reasonable effort.

7. If a hash function is used, the minimum length of the hash value shall result from the requirement in point 3.

The recommendation to carry out the pseudonymisation with the aid of a cryptographic hash function or a symmetrical block cipher procedure in which, in addition to the plaintext IDs, a secret, consistent key is used whose entropy is at least 100 bits, results from points 1.-6. Entropy is a measure of the indeterminacy of a character string (e.g. ten independent coin tosses (head/tails) provide ten bits of entropy).

5 Good Practices

Good practices have been added to this Code as a reference model and possibility to provide a better understanding of how this Code might be implemented in certain scenarios.

Following Good Practices must be considered as examples, only. There shall be no automatism that any deviation results into non-compliance with this Code. Adherent entities are being invited to refer to those Good Practices, as they are equally invited to implement alternative, but effective measures.

For the sake of a better readability and comprehensibility the following Good Practices do not use "may" or "for example" or other language indicating their exemplary character; instead, this disclaimer is being provided upfront.

5.1 Streaming Services – Large Enterprises

5.1.1 Introduction

This Good Practice presents the possible pseudonymisation process, the associated documentation procedures, and a possible distribution of roles in the context of pseudonymisation of streaming services' usage. This pseudonymisation process reflects Good Practices for companies with a complex corporate or group structure. Accordingly, the following Good Practice refers to structures that are more likely to be found in such an environment. In individual cases, smaller/medium-sized companies may have equally effective and legally compliant but deviating processes and role assignments.

5.1.2 Scope of application of pseudonymisation

The aim is to conduct analysis on pseudonymised usage data of streaming services. Such an evaluation can be used for the purpose of optimising the product (e.g., better user guidance or enhanced adaptation to end user devices). In a further step, this data is anonymised and transferred to anonymous statistics for the corresponding broadcasters. The latter is neither subject of this Code nor subject of the process described below.

5.1.3 Process specifications for the use and operation of pseudonymisation

5.1.3.1 Organisational questions

5.1.3.1.1 Designate the person responsible for the entire process

The department responsible for the streaming service is technically responsible for the pseudonymisation to be performed and therefore acts as SRP. Particularly in larger corporate structures departments take responsibility for themselves – in consultation and coordination with corporate-wide data protection and compliance departments. The latter pre-define corresponding specifications for data protection-compliant design of data processing activities. Designating the department responsible for the streaming service, which is in any case internally responsible for data protection, as responsible for pseudonymisation (SRP), reflects good practice. . In case the department has internally designated an individual person to be responsible, designating such individual person instead would follow common approaches.

In this specific Good Practice, the person responsible for pseudonymisation commissions an IT service provider with the pseudonymisation via a controller-to-processor agreement.

5.1.3.1.2 Assessment and documentation of the criteria necessary to determine the pseudonymisation method

The SRP ensures the legally compliant use of pseudonymisation and compliance with the requirements of this Code. This includes checking the legality of pseudonymisation (possibly with the involvement of a legal

department), a dedicated analysis of the data concerned, the expected cost of pseudonymisation, and the resulting considerations for the specific measures to be taken.

5.1.3.1.2.1 Type and risk class of personal data processed

Existing corporate systems for risk classification are used for the assignment to risk classes. Such classification schemes, which are usually company-wide, often consider not only data protection perspectives but also perspectives of IT security and protection of business secrets. In any case, care is taken to ensure that an existing classification offers adequate protection. Especially in complex structures, detailed differentiation is often dispensed with. Data is assigned to a formally higher protection class than strictly necessary. Thus, preference is given to a coequal high level of protection rather than complexity.

In this Good Practice, the personal data includes information on the subscriber and the device(s) used, which is enriched with user activities. These data form the basis for the pseudonymisation process. The subscriber ID and the device ID are assigned to different risk classes that have already been used in other contexts.

5.1.3.1.2.2 Intended processing purposes

In the area of analysis of streaming services, intended processing purposes of the pseudonymised data are for example

- counting adverts broadcast
- adaptations of content based on customer requirements and improved structuring of channel selection

5.1.3.1.2.3 Context of pseudonymisation

Different contexts are conceivable for the analysis of usage data. Essentially, pseudonymisation is used in this Good Practice to enable the processing purposes specified by the streaming services department. Depending on the specific offer of the streaming service, pseudonymisation may also be a necessary, risk-minimising measure in addition to the realisation of the data minimisation requirement, in particular, insofar as particularly sensitive information about data subjects is involved.

5.1.3.1.2.4 Expected number of processed records

The data sets are dynamic. More than 10 million data sets can be assumed for this Good Practice.

5.1.3.1.2.5 Suitable pseudonymisation types

There are various methods pseudonymisation types suitable to realise the intended processing purposes. In this Good Practice, cryptographic methods are considered suitable, such as a cipher method or the formation of a cryptographic checksum via the HMAC algorithm.

In the present case, a pseudonymisation method is required which can process

- a large number of data sets and
- dynamic data sets.

Information about the individual end user device can be traced (device pseudonym) as well as information about the subscriber can be traced (subscriber pseudonym). Consequently, the pseudonymisation method must be capable of initially compiling the data records to be pseudonymised from different data records (dynamically). It must also be ensured that daily findings on the same connection – even if there is a longer

break in use – can be assigned to the same pseudonym as part of a long-term evaluation. In this respect, personal pseudonyms are required for the specified purposes.

5.1.3.1.2.6 Determination of the appropriate pseudonymisation method and the time of pseudonymisation

Based on the assessment carried out in accordance with this section, this Good Practice defines a format-preserving cipher procedure as a suitable method. On the one hand, pseudonymisation is carried out continuously, namely when users carry out their activities on their streaming device (e.g., a channel change). On the other hand, pseudonymisation is performed immediately after the respective user activity.

5.1.3.1.2.7 Planned disclosure of pseudonymised data

There is no disclosure to third parties in this Good Practice.

5.1.3.1.2.8 Planned processing of pseudonymised data in the third country

In this Good Practice, no processing takes place in a third country.

5.1.3.1.2.9 Planned/ foreseeable frequency of re-identification

Re-identification is not provided.

However, users may request enhanced, individual product advice, which might require extended analysis of usage data collected. In this respect, re-identification is expected subject to specific user request – and thus based on consent.

5.1.3.1.3 Risk-adequate rights and role concept

In the present case, a great deal of data is processed. Pseudonyms are merged into profiles.

The rights and roles concepts are particularly important in this context to ensure that re-identification cannot be performed unduly. In addition, it must be ensured that those who may have access to non-pseudonymised data cannot create links by accessing the pseudonymised data at the same time.

In this Good Practice, an internal trustee model is used. The non-pseudonymised data is transferred to another "neutral" body that is spatially and organisationally separate from the specialist department responsible for the analysis. The pseudonymisation is carried out by this neutral body. The department then only receives the pseudonymised data and has no further access to relevant information that would be required for re-identification.

5.1.3.1.4 Definition of guidelines for re-identification

Re-identification takes place – if at all – only with the consent of the subscriber. Accordingly, the specifications must be clearly designed in this regard. Re-identification can only be carried out by the respective personnel if they can rely on consent at the time of re-identification. Further specifications do not appear to be appropriate in this case, as it is not assumed that the specific case will occur frequently enough.

5.1.3.1.5 Unintentional/unlawful reversal of a pseudonymisation

A corresponding process in the event of unintentional or unlawful reversal of a pseudonymisation and the assessment of a notification obligation is provided for. Such incidents are handled by the company's existing incident response system for data protection incidents. The SRP will determine the extent to which existing requirements on reporting incidents satisfy the needs in the context of the processing pseudonymised data; to the extent necessary, the SRP will work towards adapting the central requirements or supplement them with specific requirements.

5.1.3.1.6 Definition of a regular review process concerning the necessity of processing.

In this Good Practice, the generated pseudonyms are all deleted after a predefined period. There is a requirement for the specialist department to regularly check the pseudonymisation used to ensure that it still complies with the company's current specifications. From the context of the processing subject to this Good Practice, there is no need to adapt to the standardised evaluation periods otherwise valid in the company.

5.1.3.1.7 Notification obligations to supervisory authorities in special cases

There is no obligation to notify the supervisory authorities of the processing. However, in individual cases, it may appear suitable and reasonable to coordinate the pseudonymisation procedure with the competent supervisory authority.

5.1.3.1.8 Documentation and regular evaluation of the process, the considerations made, and the measures taken

5.1.3.1.8.1 Documentation of processes and other measures taken

In this Good Practice, there is a central, formalised test procedure for the pseudonymisation of personal data. For this purpose, the SRP must complete a standardised questionnaire and submit it to the technical department for review. This procedure also ensures that standardised documentation is created during and after the test, which contains the framework conditions of the pseudonymisation, and the method used. This audit is accompanied by central, documented data protection requirements for pseudonymisation.

5.1.3.1.8.2 Documentation of considerations

The considerations made and requirements for the evaluation are documented in a separate process description (see 5.1.3.1.8.1 above). It is also possible to refer to existing documents which deal with the description of the relevant processes, related requirements and measures derived from them, e.g., a prior check already carried out by the data protection officer or data protection impact assessments according to Art. 35 GDPR.

5.1.3.2 Technical questions

5.1.3.2.1 Data generation

When a streaming device is used – i.e., when the user presses the remote control – different events are generated, depending on which keys were pressed and the context in which the user does so. These events from the streaming device form the basis of the analysis. Examples of these events are, device switch-on and switch-off, channel switching, information about the channels viewed or information about activities related to recording or viewing recordings. These event records contain, for example, information about the streaming device, date/time, and other specific data fields. The personal information of these events is encrypted using a format-preserving cipher based on the AES128 (Advanced Encryption Standard with a key length of 128 bits) as a minimum.

5.1.3.2.2 Pseudonymisation

The technical procedure results in pseudonyms which are accessible to an aggregated analysis based on certain parameters. These are created using so-called deterministic, cryptographically strong ciphers. Since deterministic methods map identical plaintexts to identical result values (pseudonyms), the possibility of an aggregated analysis is ensured. Secure management of the key material as well as organisational separation of access to the keys precludes the inadmissible reversal of pseudonymisation, i.e., the disclosure of the plaintext data.

The pseudonyms, that are created for the subscriber ID and the device ID, are used for further analyses. The user activities required for analysis and the referenced subscriber ID and device ID do not contain any attributes that qualify as direct personal data.

The pseudonyms are used to collect the usage information of the streaming service to generate anonymous statistics. Here, it is important to be able to recognise which event occurs from the same device or user. Pseudonymisation ensures that employees cannot draw any conclusions about the actual devices or users. The statistics subsequently generated do not include pseudonymised identifiers anymore and, thus, are anonymous.

5.2 Optimising online platform advertising – medium-sized advertising service providers

5.2.1 Introduction

This pseudonymisation process was developed by an advertising services company to ensure protection of personal data when digital advertising is placed. Decades ago, the advertising industry developed a data protection-compliant process for playing out postal advertising in the form of the so-called lettershop process. In this process, the advertiser first determines the selection criteria for selecting data records in the consumer database. This enables the advertiser to target people who, statistically speaking, have a higher affinity for the advertised products or services than other people. The data records selected in this way are then sent to a lettershop or printing company, with the advertiser sending the print template for the direct mailing in parallel. At the service provider, the letters are printed with the addresses and sent out. The address data is then deleted. In this way, the advertiser can carry out a targeted postal advertising campaign without coming into possession of the recipients' personal data. This process is now being transferred to the digital realm.

5.2.2 Scope of application of pseudonymisation

The aim of pseudonymisation is to target an advertisement to selected consumer groups via online platforms such as social media, e-commerce stores or online publishers. The process helps advertisers to avoid placing irrelevant ads to users when playing out advertising and thus save costs. At the same time, personalised advertising saves platform users from irritation and annoyance caused by ads that are completely irrelevant to them.

5.2.3 Process specifications for the use and operation of pseudonymisation

5.2.3.1 Organisational questions

5.2.3.1.1 Designation of the person responsible for the entire process

The specialist responsible for the pseudonymisation process (SRP) is the product and engineering department, or its department head. Among other things, this department is responsible for building and maintaining the data products as well as the system infrastructure. The entire process was developed in close cooperation with the data protection department.

The individual orders for pseudonymisation of data come from internal data product owners, who execute orders from customers and partners of the company. The processing specifications as well as instructions take the form of a written commitment from a customer or partner.

5.2.3.1.2 Assessment and documentation of the criteria necessary to determine the pseudonymisation method

Following a close exchange with the data protection department, the SRP is able to ensure that the pseudonymisation procedure is implemented in compliance with data protection provisions throughout the entire process. For part of the process, the company's own Privacy Enhancement Tool (PET) is used – a pseudonymisation procedure that the company uses by default when receiving data. A separate data protection impact assessment exists for this PET, in which the legality of the pseudonymisation and the security measures to be taken were examined and affirmed as part of the balancing of interests.

5.2.3.1.2.1 Type and risk class of personal data processed

The personal data used here is only such data that was acquired specifically for advertising purposes. The data has been verified in advance as part of a due diligence process using, among other things, an existing risk classification system. As a rule, the personal data used in this process consists of the name and address and is therefore low-risk data. Nevertheless, the number of data records requires a precise internal company data protection assessment.

5.2.3.1.2.2 Intended processing purposes

The purpose of processing this pseudonymised data is the targeted placement of digital advertising on online platforms. The pseudonymisation is carried out based on a legitimate interest pursuant to Art. 6(1)(f) GDPR

5.2.3.1.2.3 Expected number of processed records

The number of data records processed corresponds to the size of the company's own address database. This database is updated on a regular basis so that, on the one hand, new data can be added and, on the other hand, objections from data subjects can be considered. The number of data processed is classified as very high.

5.2.3.1.2.4 Suitable pseudonymisation types

The suitability of the pseudonymisation types follows from various aspects of data processing. One aspect is the protection of data against unauthorised access. Even if the data categories are deemed low risk, the data records are nevertheless better protected in this way against unauthorised or unexpected third-party access. Furthermore, in this procedure, a twofold data exchange takes place: Once for creating a reference to the platform user ID and another time by hashing the personal key.

Apart from this Good Practice procedure, there is no other twofold cryptographic procedure that can be considered suitable for processing such a large number of data records on a regular basis in an interval of two to four weeks.

5.2.3.1.2.5 Planned disclosure of pseudonymised data

The pseudonymised data is transmitted to the online platform at specified intervals, thus keeping the reference file up to date. In addition, the files selected from a list of hashed personal keys for the respective advertising campaign are transmitted to the platform partner.

5.2.3.1.2.6 Planned/foreseeable frequency of re-identification

Re-identification of the data is not provided for in this procedure.

5.2.3.1.2.7 Planned processing of pseudonymised data in the third country

Depending on the online platform, it is possible that the processing takes place in a third country. In this case, however, it must be considered that the IDs in question are hashed and split IDs that can only be reversed by those who are already in possession of the plaintext data themselves and thus can create an identical data set for the purpose of matching by means of the same processing operation. Anyone who is not in possession of the initial plaintext data set cannot reverse the pseudonymisation process although reversal might be possible in general. The pseudonymised data to be transmitted will therefore be considered low risk.

5.2.3.1.2.8 Determination of the appropriate pseudonymisation method and the time of pseudonymisation

In this Good Practice procedure, two pseudonymisation methods were defined. The first is a two-stage pseudonymisation, in which data encrypted by the company's own PET hybrid process is encrypted a second

time by an encryption process supplemented with a salt (hashed personal key). In addition, the data in the address database is already only available in encrypted form. The platform operator, on the other hand, pseudonymises its own user contact data in an analogous manner, thus enabling the creation of a reference file.

5.2.3.1.3 Risk-adequate concept for rights and roles

In the present procedure, an "all-in-one-hand" model is used, in which access rights to non-pseudonymised data have been regulated by technical and organisational measures. The identification of data subjects is strictly limited by role-related access rights in accordance with the need-to-know principle.

Re-identification is not possible in this context, but there are other applications, such as address selection for mailing campaigns, where only employees of the delivery department who are responsible for delivering the data to customers or lettershops are allowed to select and deliver data records as plaintext data using pseudonymous personal keys. This conversion process is fully automated, so that the respective delivery employee merely completes the delivery file by pressing a button.

5.2.3.1.4 Definition of guidelines for re-identification

There is no re-identification foreseen in this Good Practice Procedure.

5.2.3.1.5 Unintentional/unlawful reversal of a pseudonymisation

The existing Incident Response Plan for data protection incidents also includes this Good Practice procedure. The person responsible for pseudonymisation is responsible for reporting the incident. The data protection department then carries out the risk assessment, in particular checking whether the unintentional or unlawful reversal of pseudonymisation could lead to a risk for the data subjects.

5.2.3.1.6 Definition of a regular review process concerning the necessity of processing.

The pseudonymisation procedure is required, on the one hand, as long as the relevant commercial relationship with customers and online platforms exists. On the other hand, the execution of every digital campaign requires this procedure.

Further, this procedure provides that the data immediately is deleted after a reference file has been created between the platform user ID and the company personal key, but no later than three months after the selection of records created according to the customer or partner order has been sent to the online platform partner. The storage of the delivered file is necessary for this short period, among other things, for proof in the event of a complaint by the advertiser.

For this reason, the procedure – apart from a regular review of the effectiveness of the technical-organisational measures – does not require a regular review of the necessity.

5.2.3.1.7 Notification obligations to supervisory authorities in special cases

There is no obligation to notify supervisory authorities.

5.2.3.1.8 Documentation and regular evaluation of the process, the considerations made and the measures actually taken.

5.2.3.1.8.1 Documentation of processes and other measures taken

For the pseudonymisation procedure, the person responsible for the subject created detailed documentation of the process, the test procedure, and the supporting technical and organisational measures. This information formed the basis of the data protection evaluation of the process. The person responsible for the process is responsible for compliance with and implementation of the documented specifications created by the data protection department for the process by the responsible employees.

5.2.3.1.8.2 Documentation of considerations

The considerations and specifications for the evaluation are documented in a data protection impact assessment. Stakeholders from different departments were involved to increase the objectivity of the assessment. The entire process is subject to regular external data protection audits.

5.2.3.2 Technical questions

5.2.3.2.1 Data generation

In the first step, data is matched between the address databases of the company and the platform operator. The platform operator uses its user data for pseudonymisation.

5.2.3.2.2 Pseudonymisation

The company's address databases are transferred into the PET. There, each data record of the address database receives a pseudonymous personal key. This personal key is again hashed with a salt. In addition, the company pseudonymises the plaintext data of the address database by hashing it. This creates a file with two fields: the hashed personal key and the hashed address data (match file company). The platform operator on the other side pseudonymises its user data in an analogous way and stores the hashed user contact data with the platform's own user ID in one file (match file platform). After matching the two match files based on the pseudonyms or the hash values, a reference is created between the platform user ID and the hashed personal key. The platform operator only stores the mapping of the platform user ID to the hashed personal key. All other information is deleted immediately after the matching process.

For the selection of the relevant target groups on a platform, a separate data product is created at the company, which contains the pseudonyms or personal keys as key variables, but no names or addresses.

Target groups can be selected based on sociodemographic data, calculated affinities for certain products or services, but also based on purely geographical information (e.g., advertising for high-speed Internet only in regions where it is available). The company has a wide range of microgeographic characteristics at its disposal, which are calculated on a fine-grained neighbourhood level using official data, surveys, and market research studies, etc. – (i.e., all households in a geographic cell or neighbourhood are all assigned the same values). For example, the assumption "owns a cat" is assigned to all households in this microgeographic cell, regardless of the individual situation of the different families in the neighbourhood, which must always include at least 4 households. The use of these characteristics prevents the identification of a natural person by means of these pseudonymous data sets.

The result of a target group selection (e.g., "owns a cat" and "lives in an apartment") is always a list of hashed personal keys. This is uploaded by the company to its advertising account with the platform operator and can be shared from there with the advertiser or its agency so that they can use the target group.

Based on the reference created in the data matching between the platform user ID and the hashed personal key, the platform operator switches the ad insertion in the accounts of the uploaded and shared target group.

5.3 Trustee platform for medical care and research: Developing a pseudonymisation concept

5.3.1 Introduction

The aim of the medical care and research platform is, on the one hand, to strengthen telemedical care for patients by evaluating medical data and making it available to people with a disease as part of self-management, thereby supporting them. On the other hand, product ideas from innovators are to be tested at an

early stage for their medical and health care relevance, and easier access to preclinical and clinical study facilities is to be created. In addition, research opportunities are to be offered to various stakeholders in independent science in the sense of open data sharing. Likewise, connections to professional practitioners can be created and incorporated into medication and therapy decisions based on the situation. Translating the technical possibilities and patient-generated health data into treatment successes is a central challenge of the platform.

Another fundamental feature of the platform is to evaluate pseudonymised patient data. Such an evaluation can be used for the purpose of optimising a medical product (both technical products, such as insulin pumps, and digital health applications); the processing of the data also promises deeper insights into the prospects of success of novel therapies and treatment methods, for example. In a further step, these data can be anonymised and transferred into anonymous statistics for corresponding interested parties. The latter is not the subject of the process described below.

The platform in this Good Practice is in a conceptual stage. Therefore, it shall primarily facilitate the application of the Code when selecting a suitable pseudonymisation procedure. It should be seen as an example on how to assess process specifications for the use and operation of pseudonymisation.

5.3.2 Scope of application of pseudonymisation

This Good Practice presents the possible pseudonymisation process, the associated documentation procedures, and a possible distribution of roles in the context of pseudonymisation of medical data using a trustee platform. The trustee itself is in scope of this Code, being the provider of the medical care and research platform.

The extent to which the processing of personal data via the trustee platform is permissible under data protection law is not shown via this Good Practice.

5.3.3 Process specifications for the use and operation of pseudonymisation Organisational questions

5.3.3.1 Organisational questions

5.3.3.1.1 Designate the person responsible for the entire process

In this Good Practice, the department in charge of providing trustee services is responsible for pseudonymisation. Its director acts as SRP.

5.3.3.1.2 Assessment and documentation of the criteria necessary to determine the pseudonymisation method

The specialist responsible for pseudonymisation ensures the legally compliant use of pseudonymisation and compliance with the procedure provided for in this Code. This includes checking the legality of pseudonymisation (possibly with the involvement of a legal department), a dedicated analysis of the data concerned, the expected cost of pseudonymisation, and the resulting considerations for the specific measures to be taken.

5.3.3.1.2.1 Type and risk class of personal data processed

In this Good Practice, personal data includes information about the patient and the medical device used. These data form the basis for the pseudonymisation. The patient data and the medical device identifiers are assigned to different risk classes already used in other contexts.

5.3.3.1.2.2 Intended processing purposes

Intended processing purposes of the pseudonymised data in analysis of patient data are (exemplary here from the environment of diabetology):

- Use and functional stability of insulin pumps
- Evaluations of undercutting or exceeding of threshold values
- Short-, medium- and long-term reactions to drugs and therapies
- Group and area monitoring (typing/risk clustering).
- Comparative studies (insulin A vs. insulin B; etc.)
- Combinatorial studies (such as diabetes status and dietary behaviour).

5.3.3.1.2.3 Context of pseudonymisation

Different contexts are conceivable for the evaluation of patients' personal data. Essentially, pseudonymisation is used in this Good Practice to enable the processing purposes described above while protecting the processed data from unauthorised access.

5.3.3.1.2.4 Expected number of records processed

The data sets are dynamic. An estimation of the number of data sets is not yet possible since the trustee platform is in a conceptual stage.

5.3.3.1.2.5 Suitable types of pseudonymisation

Various methods of pseudonymisation can be used for the envisaged purposes of the platform. In this Good Practice, no method is given preference, since the method to be selected is always likely to depend on the technical framework conditions or the respective legal requirements.

In the present case, a pseudonymisation method is generally required which enables the processing of

- a large number and
- dynamic data sets
- and which uses the data sets to be pseudonymised from different data sources (dynamically).

Additionally, certain information about the individual medical device (product pseudonym) and about the patient (patient pseudonym) have to be traced at a later stage. Therefore, it must also be ensured that daily findings on the same patient can be assigned to the same pseudonym within the framework of a long-term evaluation – even if the data transmission is interrupted for a longer period. In this respect, personal pseudonyms are required for the specified purposes.

5.3.3.1.2.6 Planned disclosure of pseudonymised data

A transfer to third parties, such as pharmaceutical companies, medical device manufacturers, or other authorised interested parties is planned. In principle, the data will be passed on via the data trustee, whereby each patient data record will be provided with a third-party specific pseudonym.

It could be the case that one of the data recipients, such as a medical device manufacturer, detects anomalies or the like from the data provided, in which case it would be possible to inform the patient himself/herself or his/her physician via the data trustee.

A transfer of anonymised, statistical data to third parties is also possible.

5.3.3.1.2.7 Planned/foreseeable frequency of re-identification

Re-identification is only expected upon specific request – and thus based on consent.

5.3.3.1.2.8 Planned processing of the pseudonymised data in the third country

In this Good Practice, no processing takes place in a third country.

5.3.3.1.2.9 Determination of the appropriate pseudonymisation method and the time of pseudonymisation

Based on the aforementioned, this Good Practice envisages a format-preserving cipher procedure as the appropriate method.

5.3.3.1.3 Risk-adequate rights and role concept

In the present case, a great deal of data is likely to be processed. In particular, these data – under the pseudonym – are merged into profiles. Since data sets from several medical devices may well be merged in the process, the data provider (patient) must be given the opportunity to decide which data it makes available to which physician (for example, he/she could block the visibility of data from a psychological digital health application for his treating diabetologist).

The "rights and roles"-concept is particularly important in this context to ensure that unintended re-identification cannot take place. It must be ensured that those who may have access to non-pseudonymised data cannot create links by simultaneously accessing the pseudonymised data.

Within the framework of this Good Practice, a trustee model is applied at the platform provider. The non-pseudonymised data is transferred to the trustee, which is spatially and organisationally separated from affiliated parties of the platform (such as practitioners, medical device manufacturers etc.). Pseudonymisation is carried out by the trustee. The affiliated parties then only receive the pseudonymised data and have no further access to relevant information that would be required for re-identification.

5.3.3.1.4 Definition of guidelines for re-identification

Re-identification will take place – if at all – only with the consent of the user. Accordingly, the specifications must be clearly designed in this regard.

5.3.3.1.5 Unintentional/unlawful reversal of a pseudonymisation

In the event of unintentional or unlawful reversal of pseudonymisation, a process is in place at the trustee including the assessment of a notification obligation towards supervisory authorities or controllers. Such incidents are handled by the data trustee's existing incident response system for data protection incidents. The risk of unintentional re-identification is further mitigated by an incident response process, that is aligned between the trustee and the respective controller. This includes the adoption of a "four-eyes-principle" when the trustee is approached by an affiliated party requesting the reversal of a pseudonymisation.

5.3.3.1.6 Definition of a regular review process concerning the necessity of processing.

In this Good Practice, the generated pseudonyms are all renewed after a predefined period to the effect that a new pseudonym is created for each data subject. In principle, it is then only possible for the trustee to trace pseudonyms to individuals. There is a requirement for the specialist department to regularly check the pseudonymisation used to ensure that it still complies with the company's current specifications. From the context of the processing subject to this Good Practice, there is no need to adapt to the standardised evaluation periods otherwise valid in the company. – the procedure here is based on the chaining of identities known from the trust services, as established by the eIDAS Regulation.

5.3.3.1.7 Notification obligations to supervisory authorities in special cases

There is no obligation to notify the supervisory authorities in view of the data processing.

5.3.3.1.8 Documentation and regular evaluation of the process, the considerations made, and the measures actually taken.

5.3.3.1.8.1 Documentation of processes and other measures taken

In this Good Practice, there is a central, formalised test procedure for the pseudonymisation of personal data. For this purpose, the specialist responsible for pseudonymisation must complete a standardised questionnaire and submit it to the technical department for review. This procedure also ensures that standardised documentation is created during and after the test, which contains the framework conditions of the pseudonymisation, and the method used. This audit is accompanied by central, documented data protection requirements for pseudonymisation. The procedure is to be carried out at regular intervals; the records of the audit or the documentation are kept at the Internal Audit department.

5.3.3.1.8.2 Documentation of considerations

The considerations made and requirements for the evaluation are documented in a separate process description.

5.3.3.2 Technical questions

For pseudonymisation at the trustee, a multi-stage pseudonymisation method will be used. This ensures that the patient's pseudonym and the pseudonym known to the data user (e.g., the medical device manufacturer) are never identical and can only be assigned by the trustee. Further technical aspects are not covered by this Good Practice.

5.4 Pseudonymisation software: Technical aspects of pseudonymisation

5.4.1 Introduction

While this Code is focusing on the management of process specifications for the use and operation of pseudonymisation, the technical aspects of such data transformation also play a pivotal role for protecting the rights and interests of the data subject which need to be assessed on a case-by-case basis. This Good Practice describes a scenario, where a controller or processor, subject to the Code, uses in its technical and organisational processes a software for the pseudonymisation of personal data. Therefore, this Good Practice will give examples on how to comply with Section 4.2 of the Code ("technical questions") and which other technical and organisational requirements of a pseudonymisation process such a software solution should address.

5.4.2 General functionality of pseudonymisation in the software

The pseudonymisation software will typically involve two general types of pseudonyms:

The first, are randomly assigned pseudonyms which are not generated algorithmically from the values they stand in for. Because the pseudonym itself contains no information derived from the source, there is no ability to reverse the pseudonyms.

A second type of pseudonym is often referred to as deterministic, meaning that for a specific input value, the same pseudonym always results. These have the advantage of greater analytical utility in many cases due the preservation of referential integrity but require careful consideration of the larger context within which the pseudonymised data set will be used to avoid inadvertently enabling unauthorized re-identification.

Accordingly, current state-of-the-art frameworks introduce policies for data sets as a whole by varying the details of implementation. These include fully randomised and fully deterministic policies. According to state-if-the-art software should implement at scale not only these policies but also include field, table, and database deterministic policies as well. Going further, Good Practice software enables these policies to be granularly blended and combined to fully tailor the extent to which pseudonyms are consistent or varying to allow referential integrity only when necessary to ensure the required utility, and breaking referential integrity where not required to enhance resistance to unauthorised re-identification.

In Good Practice scenarios, the pseudonymisation software is applying the following techniques:

- Allowing the user to process randomly assigned pseudonyms, albeit at the loss of any possibility of the referential integrity offered by deterministic pseudonyms, absent use of lookup tables.

- Allowing the user to generate deterministic pseudonyms generated using properly implemented secure hashing techniques, such as Keyed HMAC, which make use of indirect reversal of pseudonyms via a lookup table. Such approach is considered very robust due to the infeasibility of computing the original value from the pseudonym, or of guessing the secret key from a cleartext, pseudonym pair. The security of this approach is significantly strengthened by increased key length, as well as ensuring the security of the key and the lookup table.

- Deterministic pseudonyms generated using properly implemented secure encryption primitives which are directly reversible given access to the secret key are in general considered robust, due to the infeasibility of computing the original value from the pseudonym, or of guessing the secret key from a cleartext, pseudonym pair. The security of this approach is significantly strengthened by increased key length, as well as ensuring the security of the key.

- Sequential counters (order can leak information) and simple hash functions without a secret key, a salt or a secret “pepper” (easily defeated via brute force attacks) are considered weak techniques for generating pseudonyms and are therefore not used.

5.4.3 Identifiers and record-level protection

The pseudonymisation software is based on a data structuring framework distinguishing between different identifiers.

- **Direct identifiers**: Fields that have a one-to-one relationship with a particular data subject, and if known, allow identification of them. Examples include name, email address, national ID number, phone number, credit card number, etc.

- **Quasi-identifiers**: Fields that when used in combination, have a very high probability of allowing identification of a data subject. Examples include Art. 9(1) GDPR special category data, sex, birthdate or age, postal code, and location data (especially if high resolution or over time).

- **Indirect identifiers/attributes**: All other fields in a data set. Historically, indirect identifiers were distinguished as fields that in combination might lead to identification, and attributes were other values of little use in identification. However, with the rise of massive amounts of easily obtainable outside data source, nearly all fields in a data set can be leveraged for re-identification given the right external data. Thus, it is appropriate to treat these two categories the same from a re-identification risk perspective.

The following methods are applied to identifiers to achieve GDPR pseudonymisation:

5.4.3.1 Direct identifiers

- Consistent with the principles of data minimisation and the obligations of data protection by design and by default, unless required for processing, direct identifiers are excluded from the output.
- If one or more must be included, they are replaced with a pseudonym using a randomly assigned value if possible.
- Short of that, as many characters as possible are masked or replaced using a deterministic pseudonym, based on the requirements of the processing.

5.4.3.2 Quasi-identifiers, indirect identifiers, and attributes (i.e., all other fields)

- Consistent with the principles of data minimisation and the obligations of data protection by design and by default, unless required for processing, all other fields of the underlying database are also excluded from the output.
- Fields that are categorical/nominal (e.g., gender, postal code, age ranges, etc.) or than can be converted into nominal (through the creation of ranges or binning, or the use of dummy variables or so-called "one-hot encoding") should be pseudonymised. While in theory these might be random pseudonyms, in practice they will most commonly be deterministic. The key consideration is the scope of the determinism. In compliance with data protection by design and by default, the first option will be field deterministic, where the pseudonyms are consistent within a single column. Next will be table deterministic, followed by database deterministic. And finally, fully deterministic. Each succussive expansion of scope will increase the risk of unauthorised re-identification from the potential for combining disparate sources of data and therefore must be subject to a use case specific risk assessment.
- Fields that are natively categorical/ordinal or numerical/interval are evaluated to assess whether the process requirements can be satisfied by transforming them into nominal by replacing them with deterministic pseudonyms and converted back to clear-text ordinal or interval post processing via relinking using the information held separately. If they must remain ordinal or interval, where possible they should be transformed using ranges, binning, or rounding.
- Fields that are natively numerical/ratio are evaluated to assess whether the process requirements can be satisfied by transforming them into nominal, though it will not be common for that to be the case. More typically they will need to be retained as at least ordinal or interval. In practice, however, in most cases they will likely need to be retained as interval, with some needing to be included untransformed and others transformed using ranges, binning, or rounding.

5.4.3.3 Record-level protection

- The forgoing protections ensure strong resistance to unauthorised re-identification from linkage and inference attacks, but only limited protection against attacks based on singling out[5], which is essential in ensuring that that the data set meets the GDPR´s requirements for pseudonymisation.
- An effective approach for addressing singling out is to evaluate the protected data set using k-anonymity scored against quasi-identifiers and suppressing records that fail to meet the specified level of k[6].

[5] See https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf Section 3 for a discussion of these attack vectors.

[6] See ibid at Section 3.2.1 for an introduction to k-anonymity.

5.4.4 Planned/foreseeable frequency of re-identification

Pseudonymisation implemented using the types and methods noted above can be implemented at scale in a manner that facilitates controlled re-identification for authorised use cases, whether for limited or extensive subsets of the data, and whether re-identification is authorised infrequently or routinely.

5.4.5 Risk-adequate concept for rights and roles

Careful consideration should be given to how many of the various components that form the pseudonymisation process any single individual can access. Good practice starts with the principle that it should be limited to only those necessary to fulfil their role. Likewise, account must be taken for the risk of unauthorised re-identification resulting from the selected combination. The pseudonymisation software uses the following components subject to access control:

- Data source schemas including metadata
- Data sources
- Configuration settings for creating pseudonymised data sets
- Digitised privacy polices
- Pseudonymised datasets
- Information necessary to relink pseudonyms to data subjects

And actions that may be performed on them:

- Read
- Create
- Modify
- Share
- Delete
- Start processing
- Stop processing

6 Monitoring and Compliance

6.1 Introduction

This Section governs all provisions related to the appointment of the Monitoring Body, adherence of pseudonymisation processes (PPs) to this Code, compliance of adherent PP, and the monitoring of and complaints' handling under the Code.

6.2 The Monitoring Body

6.2.1 Appointment, Revocation and Suspension of the Monitoring Body

6.2.1.1 Appointment

Acknowledging the requirements of Art. 40 and 41 GDPR, only entities which are accredited as a monitoring body can be appointed by the Steering Board, as Monitoring Body of this Code. Until the appointed Monitoring Body has no accreditation pursuant to Art. 41 GDPR, this Monitoring Body shall not verify any pseudonymisation process as compliant with this Code as a code of conduct pursuant to Art. 40 GDPR.

6.2.1.2 Revocation and Suspension

The Steering Board shall suspend or revoke the appointment of the Monitoring Body whenever the Monitoring Body loses its accreditation. In other circumstances the Steering Board shall only suspend or revoke the appointment of the Monitoring Body in cases where the Monitoring Body is grossly negligent in its responsibilities, e.g., by gross misconduct or fraud. A revocation or suspension of the appointment of the Monitoring Body for other reasons shall only be performed under consultation with the competent supervisory authority and with a prior notification of the Monitoring Body of at least 18 months. If and to the extent the Steering Body decides to revoke or suspend the Monitoring Body, the Steering Board shall promptly and duly – i.e., prior to the final suspension or revocation – notify the Monitoring Body's competent supervisory authority.

6.2.1.3 Consequences of Revocation and Suspension

If the Steering Board suspends or revokes the appointment of the Monitoring Body, the Steering Board shall notify the Monitoring Body's competent supervisory authority prior to any such decision. The Steering Board then shall – in consultation with the competent supervisory authority – take appropriate actions.

6.2.1.4 Consequences of cease to exist in law of the Monitoring Body

If the Monitoring Body runs bankrupt or otherwise ceases to exist in law, the procedure of 6.2.1.3 shall apply accordingly.

6.2.2 Functions of the Monitoring Body

The appointed and accredited Monitoring Body (6.2.1.1) Art. shall perform the following operational duties:

- Review and verify compliance of PPs with the Code;
- Regularly monitor whether adherent PPs are compliant with the Code;
- Review and decide complaints about infringements of the Code by adherent PPs;
- Establish procedures and structures to deal with complaints about infringements of the Code or the manner in which the Code has been, or is being, implemented by Signatories, and transparently communicate these procedures and structures;
- Implement procedures and structures that prevent conflicts of interests;
- Take appropriate action, selecting from sanctions laid down in 6.9 or, where applicable, from the Guidelines as adopted by the Steering Board (see 7.1.2), against a Signatory in case of an infringement of the Code or in case a Signatory is not providing the information necessary to review a possible infringement of the Code to the Monitoring Body;

- Inform the competent supervisory authority of actions taken against Signatories and the reasons for taking them (see6.9.4).

6.2.3 Minimum safeguards with regards to policies, procedures, and structures

Without prejudice to the accreditation pursuant to Art. 41 GDPR the Monitoring Body shall develop and implement appropriate policies, procedures and structures to:

- Ensure independence and expertise in relation to the Code, for instance a minimum period of appointment, expertise of its personnel and of the members of the Complaint's Committee;
- Allow verification of compliance for PPs and to regularly monitor whether adherent PPs are compliant with the Code;
- Handle complaints about any potential non-compliance of an adherent PP with the Code;
- The Monitoring Body will appoint an independent Complaints Committee (6.9.1);
- Ensure internal separation of duties within its structures, including the Monitoring Body's unit to verify and monitor PPs compliance to the Code and the Complaints Committee;
- Prevent conflicts of interest, implementing, for example, safeguards that complaints and declarations of adherence or any periodical reviews are decided by different individuals;
- Ensure that, according to the requirements of the respective Compliance Mark, periodic reviews cover all requirements of the Code within a reasonable period;
- Ensure that expertise of individuals working for the Monitoring Body, including members of the Complaints Committee, is proven by relevant academic degrees, several years of relevant working experience and/or relevant publications.

The Monitoring Body shall make the referred policies, procedures, and structures public and available on its website.

6.2.4 Confidentiality of the Monitoring Body

The Monitoring Body is allowed to use the information obtained during a review process only for purposes related to its responsibilities pursuant to the Code. The Monitoring Body including any persons working on their behalf, is bound by an obligation of confidentiality, and ensures that all information received in the context of its activities shall be kept undisclosed and adequately protected from unauthorized access and shall be deleted when no longer necessary for the purpose it was obtained, unless otherwise determined by applicable mandatory law.

6.2.5 Transparency and Documentation obligations of the Monitoring Body

Any decision or action taken by the Monitoring Body shall be documented. Such documentation shall include, at least, the decision or action, date, substantial and essential circumstances in which such decision or action were based, main reasoning and individuals responsible. This documentation shall be kept for the time a Signatory is adherent to the Code plus any suitable period to safeguard the performance of powers of supervisory authorities related to Art. 40 and 41 GDPR, provided that there is no conflict with the applicable legislation of the Member State of the Monitoring Body or its competent supervisory authority (whatever is the longer period). Any further details may be governed by specific procedures of the Monitoring Body in consultation with the competent supervisory authority.

Upon request of the Monitoring Body in accordance with its duties and competences under the Code, Signatories will cooperate with the Monitoring Body providing relevant information to the Monitoring Body. Breach of such obligation could amount to an infringement of the Code.

6.3 Conditions of Adherence

Signatories that consider one or more of their PPs to meet the requirements set out in the Code, can submit a declaration of adherence of one or more of their pseudonymisation processes, to the Monitoring Body and follow the procedure set out in this Code.

By submitting a declaration of adherence of pseudonymisation processes to this Code, the Signatory commits to comply with the requirements of the Code for any pseudonymisation processes covered by its declaration. Any PP to the Code must comply with all requirements of the Code and not only parts of the Code.

Verified adherence of pseudonymisation processes to the Code does not absolve any Signatory from having to comply with the GDPR, and/or applicable EU Member State data protection law, nor does it protect Signatories from possible interventions or actions by supervisory authorities in the course of their supervision and enforcement activities with regards to the adherent PPs. GDPR and applicable Member State Law will always prevail over the Code.

PP will undergo rigorous scrutiny by the Monitoring Body, in accordance with the requirements stipulated by this Code and / or the Monitoring Bodies procedures as accredited by the Monitoring Body's competent supervisory authority.

Without prejudice to sanctions from competent authorities as foreseen in case of breaches of the GDPR and/or other legal acts, any Signatory, which fail to meet the requirements of the Code, will be subject to the enforcement mechanisms as set out in this Section of the Code.

6.4 Procedure to declare a PP adherent

Signatories submit their declaration of adherence to the Monitoring Body following the procedure provided by this Code. The procedures published by the Monitoring Body may determine that a submitted declaration of adherence shall be received only by utilizing distinct templates or online forms. Any declaration of adherence, however, shall at least entail the following information:

- identification of the PP
- name of the Signatory that provides such PP
- contact details of the Signatory
- a legally binding statement that the PP is fully compliant with all requirements of the Code

Upon request by the Monitoring Body, the Signatory shall provide information relevant for the declaration of adherence in an up-to-date and accurate manner. A Signatory shall notify the Monitoring Body promptly whenever information provided within the declaration of adherence becomes outdated or inaccurate, regardless of its reason. Providing outdated or false information could amount to an infringement of the Code. The lack of notification shall be treated as providing outdated or inaccurate information.

The Monitoring Body shall review the declaration of adherence in due time. Once verified, the verified pseudonymisation processes shall be incorporated into the public register. The public register shall at least provide the following information:

- Pseudonymisation process adherent to the Code;
- Date of verification of compliance;

A Signatory whose declared pseudonymisation process was not verified compliant by the Monitoring Body may submit a revised declaration of adherence and information, subject to the fees as approved by the General Assembly or file a complaint pursuant to Section 7.3.4.

6.5 Assessing compliance with the Code

To ensure that the Monitoring Body and supervisory authorities can verify that the requirements of this Code are met by the PP, the requirements of this Code are referred to by the pattern 'Section, Paragraph'.

For the avoidance of doubt: Wherever this Code makes use of the terms "shall" and "must", a Signatory is obliged to implement the respective provision to be compliant with this Code. Wherever this Code makes use of the terms "should", "may" or "can", the Code introduces examples and recommendations. Regarding Section 5 "Good Practices" those shall always provide non-binding examples, regardless of any terminology used therein.

6.5.1 Explanation and Good Practices

The Code also introduces explanations and Good Practices, Section 5. Explanations and Good Practices are a selection of good practices on how the Requirements they relate to can be implemented by Signatories declaring a pseudonymisation process adherent to this Code.

The Explanation as well as Good Practices and the original requirements of the Code shall be considered by the Monitoring Body when verifying the compliance of a PP to the Code. Neither Explanation nor Good Practices are mandatory. If a Signatory implements alternative measures to be compliant with this Code, these measures must not be less protective than those being provided by the Explanation or Good Practices.

6.5.2 Assessment by the Monitoring Body

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant Art. 41 GDPR, the Monitoring Body shall assess whether a pseudonymisation process is compliant with the requirements of the Code.

Unless provided otherwise by the Code, the Monitoring Body assessment process shall be based on an evidence-based conformity assessment, based on interviews and document reviews; pro-actively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a Signatory with regards to the pseudonymisation process, the Monitoring Body may request additional information.

Where the information provided by the Signatory appears to be inconsistent or false, the Monitoring Body shall – as necessary – request substantiation by independent reports; costs related to such substantiation shall be covered by the Signatory.

If and to the extent the Code or a Requirement leaves room for interpretation, the Monitoring Body shall provide the final conclusive decision, whether the Code's requirement is being complied with. The Monitoring Body shall consider any notion provided by the Code language and as noted in 6.5.1 by Good Practices and Explanations.

6.6 Compliance Marks

6.6.1 Entitlement to use Compliance Marks

Signatory is entitled to use the Compliance Mark provided that the respective PP has been both verified compliant by the Monitoring Body and has been listed in the Public Register.

If after being verified compliant by the Monitoring Body, a dispute concerning non-compliance of such PP arises, the Signatory is entitled to continue using the Compliance Mark until the Complaints Procedures pursuant to Section 6.8.2. comes to a resolution. After receiving a final outcome of non-compliance with the Code of the adherent PP concerned, the Signatory must immediately cease to use the Compliance Mark with regards to those pseudonymisation processes if imposed accordingly by the Complaints Committee pursuant to Section 6.9.2. Misuse of Compliance Marks will amount into an infringement of the Code.

6.6.2 Use and communication of Compliance Marks

Regarding PPs that are verified compliant the Signatory shall integrate the Compliance Mark in its communication towards data subjects of the respective pseudonymisation process, e.g., its communication related to compliance with international standards. The Compliance Marks shall only be used in combination with the unique Verification-ID assigned by the Monitoring Body. Where technically possible, the Compliance Mark shall link to the public register of the Code; otherwise, the Signatory shall provide at least a footnote with a reference to the public register. In consultation with the Steering Board the Monitoring Body shall provide further details and templates regarding the use and communication of Compliance Marks to prevent any confusion of the market. Breach of the aforementioned provisions could amount into an infringement of the Code.

6.7 Monitoring and enforcement

6.7.1 Monitoring

The compliance of any pseudonymisation process that has been declared its adherence to the Code will be monitored by the Monitoring Body. While this Code provides the material criteria, the processes on how the monitoring will be performed shall be governed by accredited procedures of the Monitoring Body. Notwithstanding, at a minimum every Signatory shall provide the Monitoring Body once a year with an overview and reference to existing documentation as required by this Code, allowing the Monitoring Body to verify completeness and selection of an adequate sample of Signatory for in-depth assessments.

Compliance of adherent pseudonymisation processes shall be reviewed every twelve months unless

a) any significant changes occur to adherent pseudonymisation processes,

b) in reaction to a complaint, an adverse media report or anonymous feedback about a Signatory which has declared a pseudonymisation process adherent to the Code;

in which case the PP shall be reviewed earlier.

Not submitting the compulsory annual renewal of a declaration of adherence shall be considered as infringement of the Code if to the extent the Signatory has not terminated its adherence consistent with the provisions of this Code and the procedures established by the Monitoring Body.

6.7.2 Enforcement

If the Monitoring Body becomes aware of any non-compliance of an adherent pseudonymisation process, the Monitoring Body can request the Signatory to take specific measures ceasing any further infringement by the respective pseudonymisation process. Therefore, the Monitoring Body shall notify the Complaints Committee, which then shall take the appropriate action with regards to the sanctions and remedies pursuant to Section 6.9; this procedure only applies if the pseudonymisation process is listed as current and verified as compliant.

If the verification of compliance of a pseudonymisation process is revoked, the pseudonymisation process shall be deleted from the public register; the Monitoring Body shall inform the competent supervisory authority accordingly. The Signatory shall cease to use the Compliance Mark with regards to the respective pseudonymisation process in any of its documentation or publications, including its website, or any other communication creating the wrongful impression of compliance with the Code.

6.8 Complaints Handling and Procedures

6.8.1 Complaints of Signatories against decisions of the Monitoring Body

Signatories may file a complaint against any decision taken by the Monitoring Body.

Complaints against any rejection of the verification of compliance with the Code shall be addressed to the independent Complaints Committee of the Monitoring Body. The independent Complaints Committee, see Section 6.9.1, re-assesses the compliance of the declared Pseudonymisation process based on the information presented to the Monitoring Body and either verifies the Pseudonymisation process compliance or confirms the prior rejection.

6.8.2 Complaints against any Signatory and its pseudonymisation process' compliance

The data subject and any other party can submit a complaint to the Monitoring Body at any time, also anonymously.

The Monitoring Body shall review the complaint, require the Signatory to provide any relevant information for the purposes of fact finding, and initiate a complaint handling process, in which its independent Complaints Committee, see Section 6.9.1, will determine whether the complaint was justified. In case the Complaints Committee concludes that the complaint was justified the Monitoring Body will in accordance with the Complaints Committee take appropriate actions to stop any further non-compliance of the adherent Signatory.

The Complaints Committee will process complaints, establish whether violations of the Code have occurred and decide on possible sanctions and remedies in accordance with the sanctions and remedies provided under this Code.

Subject to the accreditation by the competent supervisory authority, the Monitoring Body may define further detailed procedures governing complaints handling. Such procedures shall be publicly available.

6.8.3 Costs and Fees related to Complaints

6.8.3.1 Costs for Complainants

As a rule, complaints can be submitted free of costs. However, the Monitoring Body may define costs for complainants, where appropriate, to avoid abuse due to manifestly unfounded or excessive complaints, in

particular if they are recurring. In such cases the Monitoring Body may charge a reasonable fee related to its administrative costs, or simply refuse to act on the complaint. The Monitoring Body shall be able to reason its actions related to the manifestly unfounded or excessive character of the request and – subject to the accreditation of the competent authority – appropriately notify the competent authority of such cases.

6.8.3.2 Costs for Signatories – Rule

The costs for the performance of the Complaints Committee, i.e., the general complaints handling such as validation, internal preparation and postprocessing of Complaint's Committee meetings, and reasonable fact finding, shall be covered by the service fees paid by Signatory to the Monitoring Body.

Additional costs which are deemed necessary by the Monitoring Body, shall be borne by the Signatory whose PP is concerned. Such additional costs may include on-site reviews, or third-party reports, travel expenses.

6.8.3.3 Costs for Signatories in case of justified complaints

If a complaint is justified in accordance to 6.8.1 and 6.8.2 by the Complaints Committee, the applicable Signatory shall pay the costs that result from handling of such Complaint, including those costs that would be covered by the service fees. In those cases, the Complaint may be subject to fees, which shall be cost-based pricing and approved by the General Assembly.

The General Assembly may – in consultation with the Monitoring Body – decide upon a fixed Complaints Fee; if the General Assembly decides upon such fees, they shall be reviewed annually to ensure that the Complaints Fee mainly covers the overall costs of the Monitoring Body and its Complaints Committee. The applicable Signatory shall cover the complaints costs without prejudice to other potential sanctions imposed by the Monitoring Body and its Complaints Committee, pursuant to Section 6.9.

6.9 Sanctions, remedies, and notification of the supervisory authority

The Monitoring Body shall take appropriate actions against any Signatory whose PP is non-compliant with the requirements of this Code or who refuses or fails to cooperate appropriately with the Monitoring Body under this Code and GDPR. Those powers are notwithstanding the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII GDPR. Appropriate actions are considered those as defined as sanctions and remedies in this Section of the Code.

6.9.1 Independent Complaints Committee

To prevent any conflicts of interests the Monitoring Body shall establish an independent Complaints Committee, by which the Monitoring Body safeguards that the same personnel will not decide upon its own, prior assessments and decisions. The Complaints Committee shall document the facts found by the Monitoring Body, the reason to consider that facts result in non-compliance of the Code, every action taken and an explanation for such action taken.

6.9.2 Sanctions and Remedies

If a PP to this Code is non-compliant with any requirement of the Code, the applicable Signatory shall be subject to appropriate actions. By imposing any action, the Monitoring Body shall consider the following aspects when assessing the appropriateness of each action:

- severity of non-compliance with regards to the potential impact on level of data protection related to the personal data processed, including the potential impact on the freedoms and rights of data subjects;

- culpability of the Signatory – whether the Signatory intentionally or negligently disrespected the requirements of the Code;
- frequency of non-compliance – has it been the first breach or have there been similar incidents before.

Based on the aforementioned criteria the Monitoring Body shall impose sanctions and remedies that can be one or any combination of the following:

- non-public but formal reprimand;
- public announcement of the non-compliance, including facts and reasoning;
- temporary or permanent revocation of the verification of compliance with the Code related to the PP concerned;
- temporary or permanent revocation of the verification of compliance with the Code related to all PP of the Signatory;
- temporary or permanent revocation of membership in the General Assembly.

6.9.3 Guidelines for Sanctions and Remedies

Where appropriate and to subject to its sole discretion, the Monitoring Body shall draft, approve, and frequently review supplementary Guidelines for Sanctions and Remedies ("**Guidelines**"). The Monitoring Body shall consider its practical experiences regarding to non-compliance of Signatories and their pPP. Those supplementary Guidelines shall safeguard comparability and coherency of sanctions and remedies imposed to Signatories. The Monitoring Body shall consult the Steering Board when drafting such Guidelines. The Guidelines shall at least enlist and name the individual aspect of non-compliance as well as the sanctions and / or remedies to be expected. The determination of sanctions and remedies shall be chosen from the potential sanctions mentioned in this Code as well as those aspects to be considered by the Monitoring Body to assess the appropriateness of any sanction and remedy, for both see Section 6.9.2.

To the extent not already covered by the procedures as defined by the Monitoring Body to receive its accreditation pursuant Art. 41 GDPR, such Guidelines shall also cover appropriate periods of response and implementation of imposed remedies, including consequences of non-compliance with such periods by Signatories and appropriate actions and timeframes for escalation of sanctions.

To prevent any conflicts with the independence of the Monitoring Body, the Monitoring Body shall take such Guidelines into account when imposing any action against a Signatory. If the Monitoring Body considers its guidance as inappropriate it may deviate, provided that the Monitoring Body documents appropriate reasoning why such deviation seemed inevitable. Such a decision shall result in a review of the Guidelines.

6.9.4 Notification of and cooperation with the supervisory authorities by the Monitoring Body

Without prejudice to Art. 41.4 GDPR, the Monitoring Body shall proactively and in due time notify the competent supervisory authority of sanctions and remedies imposed on Signatories and the reasons for taking them, including non-public but formal reprimands.

In cases any supervisory authority concerned reaches out to the Monitoring Body that actions taken by the Monitoring Body frequently remain behind what supervisory authorities expect as appropriate action, the Monitoring Body will take this feedback into account for any future decision to be taken. Especially to the extent supervisory authorities frequently reach out to the Monitoring Body related to the same field of

action, the Monitoring Body shall – to the extent possible – adjust its procedures and internal guidelines accordingly. To the extent the Monitoring Body cannot adjust its procedures or internal guidelines accordingly, e.g., as such adjustments require modifications to the Code, the Monitoring Body shall reach out to the competent body within the Code.

7 Internal Governance

This Section of the Code intends to enable a sustainable model of governance at multiple levels:

Firstly, the governance of the organisational framework of the Code itself and its bodies, through a General Assembly and a Steering Board with operational decision-making power Secondly, the governance of the Code itself, ensuring that it can be updated to reflect the GDPR and ensuring that lessons learned in the interpretation and application of the Code can be appropriately integrated.

This governance system is envisaged to be put in place progressively and in a transparent way, building on the input of relevant stakeholders. Organisations interested in being part of the governance will be invited to express their interest to the General Assembly.

7.1 Organisational framework of the Code and its bodies

The Code Governance Bodies are tasked with the implementation and administration of the Code.

7.1.1 Code General Assembly

7.1.1.1 Composition and representatives

The General Assembly is composed of all members, whose applications to join have been approved by the General Assembly, provided that each of the members (the "**Members**"):

- have at least one PP adherent to the Code;
- provide operational support to the Code as agreed by the General Assembly;

Each Member of the General Assembly is entitled to one vote, even though Members may be represented by more than one individual, which should have expertise in pseudonymisation and/or data protection. Each Member shall inform the Chairperson of the General Assembly, prior to each General Assembly Meeting, of who their representatives are.

A Signatory may cease to be a Member of the General Assembly, by giving the Secretariat 3 (three) months prior notice, copying the Chairperson of the General Assembly, where applicable.

7.1.1.2 Powers

The General Assembly may designate the Chairperson of the General Assembly including up to two Vice Chairpersons and shall have the powers

- to define and approve annual membership fees, Supporter fees and any other fees as proposed by the Steering Board;
- to approve new Members;
- to decide on temporary or permanent revocation of membership within the General Assembly following unremedied breach of the Code which is not a breach of Section 4;

- to approve changes to the Code as proposed by the Steering Board, and
- to decide on or approve any other matters as proposed by the Steering Board.

7.1.1.3 Chairperson of the General Assembly

The Chairperson of the General Assembly and its Vice Chairpersons shall be elected by the General Assembly for a term of two years, with the possibility of renewing its mandate for any number of successive additional two-year terms.

7.1.1.4 Convene the General Assembly

A General Assembly Meeting may be convened, on first call, by email sent with at least three weeks' prior notice and, on second call, by email sent with at least one weeks' prior notice.

A Member of the General Assembly shall be deemed to have been properly notified if the notice is sent to the email address, which the Member had beforehand registered at the Secretariat.

The Chairperson shall convene one annual General Assembly Meeting, during the first quarter of each civil year. The Chairperson shall also convene a General Assembly Meeting, upon request of any Member of the General Assembly, as well as upon request of the Steering Board or the Monitoring Body, which must clearly state in writing the matters of the agenda and the purpose of the meeting.

The decisions to accept new Members may be taken through email, without the need to convene a General Assembly Meeting. The decision shall be considered approved if, after ten days of receiving the request for approval through email, the Members either approve or are silent. If a Member rejects accepting a new Member, then the Chairperson of the General Assembly shall convene a regular General Assembly Meeting in accordance with the previous paragraphs.

7.1.1.5 Meeting

The Members may participate in a General Assembly Meeting either physically or remotely via electronic meetings or conference calls, allowing all Members, participating in the meeting, to always hear each other and at the same time.

The General Assembly may request experts to provide information on relevant topics or to attend meetings as invited guests to their deliberations.

7.1.1.6 Quorum and majorities

The General Assembly's resolutions may only be validly taken with a majority of the votes cast provided that fifty percent of the Members of the General Assembly are present or represented. However, if there is not a quorum present when a meeting is first called, a simple majority of those present or represented at an adjourned meeting will suffice to approve the resolution.

The members of the General Assembly may pass unanimous decisions in writing, including email, or hold a General Assembly Meeting without any prior formalities, provided always that all Members are present and express their agreement.

7.1.1.7 Representation

At a General Assembly Meeting, members may be present or represented. To be represented includes the possibility to assigning another Member of the General Assembly as proxy or to submitting any votes upfront to the Secretariat in writing, including email. One Member must not hold more than two proxies.

7.1.1.8 Challenging Decisions

Members may challenge decisions within eight weeks after the minutes of a General Assembly Meeting or any decision have been provided. Provided Members were present or represented at the General Assembly Meeting they shall only be entitled to challenge formal requirements if they have risen concerns during the General Assembly Meeting. Provided Members were not present or represented at the General Assembly Meeting but properly notified, Members shall not be entitled to challenge any decisions unless it is related to a breach of formal requirements during the course of a General Assembly Meeting.

7.1.2 Code Steering Board

7.1.2.1 Composition and members

Members of the Steering Board shall be appointed by the Chairs of the Steering Board. The Chairs of the Steering Board shall ensure that each individual being appointed as Member of the Steering Board has proven expertise in the area of pseudonymisation and / or data protection.

As a rule, the Steering Board shall be comprised of representatives of Signatories. Therefore, representatives of Signatories are encouraged to apply to become Member of the Steering Board. Additionally, Steering Board Chairs may invite interested third parties to join the Steering Board and appoint them as Member with a view of strengthening the balanced representation of stakeholders interested in participating in the Code, from both the private and public sectors.

Steering Board Chairs shall ensure that the Steering Board will at least comprise of sixty percent (60%) representatives of Signatories.

Notwithstanding the above, the Steering Board may invite and consult experts, where necessary.

Should the need arise, in view of the future evolutions of the Code, the Steering Board may decide to appoint a drafting team of qualified experts to prepare amendments to the Code.

7.1.2.2 Representation

At a Steering Board meeting, members may be present or represented. To be represented includes the possibility to assigning another Member of the Steering Board as proxy or to submitting any votes upfront to the Steering Board Chairs in writing, including email. One Member must not hold more than two proxies.

7.1.2.2.1 Powers and Functions

The Steering Board, directly or through any subcommittees it chooses to create, performs the following powers and functions:

- Monitor changes in European Union data protection laws
- Monitor issues and new developments impacting the Code, where necessary by establishing and proposing an annual work programme in consultation with the supervisory authorities, the European Data Protection Board and Commission
- Define and propose amendments to the Code for approval by the General Assembly. The Steering Board shall aim to propose relevant changes to the Code within six months in case of material changes in European Union data protection laws, taking into account the extent and complexity of the changes;
- Define and propose amendments to the governance of the Code for the approval of the General Assembly;

- In consultation with the Monitoring Body, define and propose templates and online forms for the submission of the declaration of adherence to the Monitoring Body;

- In consultation with the Monitoring Body, define and propose minimum requirements for the assessment of declarations of adherence by a Monitoring Body;

- Define and propose more detailed guidelines for the application and interpretation of the Code considering any feedback of the Monitoring Body. Such guidelines must not, however, lower the level of data protection as provided by the present Code or materially change the Code. and will, always, ensure compliance with the GDPR. However, to adequately align with the competent supervisory such guidelines and any modification thereof shall be presented to the competent supervisory authority prior publication to enable the supervisory authority to request formal approval pursuant to Art. 40 GDPR, where considered necessary.

- Define and propose more specific modules to the Code, e.g., in relation to specific use cases, data types, service provisioning models, sectors or industries; such modules shall be submitted to the competent supervisory authority for approval pursuant to Art. 40 GDPR, without limiting any powers and deviating interpretation of supervisory authorities;

- Adopt Compliance Marks that may be used by adhering Members;

- Appoint the Monitoring Body and withdraw or suspend the appointment in case of factual indications that the Monitoring Body no longer meets the requirements defined in this Code. A Competent Monitoring Body shall only be appointed by the Steering Board, after the Steering Board has determined that the Monitoring Body is capable of performing the functions referred in Section 6.2.2, and fulfils the following criteria to the satisfaction of the Steering Board:

  - has established procedures which allow it to assess the eligibility of Signatories to declare their Pseudonymisation processes adherent to the Code;

  - to monitor Signatories and their adherent PP compliant with the Code's provisions, and

  - to periodically review the Signatories operation if needed;

- Discuss and submit for the approval of the General Assembly, membership fees, Supporters fees and, in consultation with the Monitoring Body, fees for declaration of adherences and their reviews, complaints fees, and any other fee that might be applicable;

- Propose, for the decision of the General Assembly, a list of sanctions and remedies, to be imposed by the Monitoring Body, in case of an infringement of the Code. Those shall include, e.g., the suspension or exclusion from the Code, and the publication of such decisions taken by the Monitoring Body. This goes notwithstanding and to no means limiting any legal obligation of the Monitoring Body to publish certain decisions;

- Adopt, for the decision of the General Assembly Guidelines for the application of sanctions and remedies, see Section 6.9.3;

- Approve the Secretariat, selecting a suitable organisation to perform the Secretariat tasks on the basis of non-discriminatory and objective criteria.

Any decisions or proposals shall be approved by the General Assembly to become effective.

7.1.2.3 Chairs of the Steering Board

GDD and Bitkom shall each designate one Chair among their staff or member associations for a period of two years, with the possibility of renewing their mandate for any number of successive additional two-year terms.

7.1.2.4 Convene the Steering Board

Meetings of the Steering Board shall be held at regular intervals, each meeting convened by the Chairs of the Steering Board. Minutes of such meetings shall be prepared, as soon as practicable following such meetings. There should be a minimum of 2 (two) meetings of the Steering Board in each year.

Notice in writing of not less than three weeks, on first call, and one week on second call, shall be given to each Steering Board Member of every proposed meeting of the Steering Board accompanied by an agenda specifying, in reasonable detail, the matters of the agenda. In cases of urgent need, e.g., where the Code needs to be adapted to comply with an updated legal framework or any interpretation thereof, the Steering Board can be convened with short notice of five days on first call, and one day on second call; whenever this provision shall apply, it shall be transparently indicated and referred to in the notification of convention.

Any Member of the Steering Board shall have the right to call a meeting of the Steering Board at any time.

A meeting of the Steering Board may be convened on shorter notice provided that all the members of the Steering Board consent to such shorter notice.

7.1.2.5 Meeting and members' representatives

Each Member of the General Assembly shall procure that their respective appointees to the Steering Board attend each meeting of the Steering Board and they each shall use their best endeavours to procure that a quorum is present throughout each meeting of which due notice has been given.

The members may participate in the Steering Board either physically or remotely via electronic meetings or conference calls, allowing all representatives participating in the meeting to hear each other, at all times, and at the same time.

Provided that copies of all relevant documents are first sent to all the members of the Steering Board, a resolution of the Steering Board may also be taken without a meeting if it is agreed and documented by all members of the Steering Board.

Meetings of the Steering Board shall take place on the date and at the time designated in the notice of the meeting.

7.1.2.6 Quorum and Majorities

The quorum for all meetings, at first call, of the Steering Board shall be a simple majority of votes of all the members of the Steering Board. If a meeting is not quorate, it shall be adjourned to a date at least one day after the date of the first meeting. The quorum for a meeting adjourned shall be a simple majority of the members of the Steering Board present or represented.

Provided there will be more than one representative per Signatory, not more than one vote per Signatory shall be considered valid and due.

7.1.2.7 Disputes amongst Members

The Steering Board shall develop appropriate policies to assure that interests are disclosed, and conflicts are avoided between Members. Mechanisms will include separation of duties, recusal or other policies

undertaken by the Steering Board, and the possibility for the General Assembly to raise objections against individual Steering Board members. The Steering Board will also create an impartial mechanism to hear and decide on conflicts as well as appropriate appellate procedures related to decisions that impact organisations or competent bodies.

Without prejudice to the powers and capacity of the Monitoring Body, the Steering Board may propose to the General Assembly to temporarily or permanently suspend or revoke the membership status of any Member of the General Assembly due to infringements against the governance of this Code.

7.1.3 Code Supporters Licensors

7.1.3.1 Supporters

Separately and without obtaining voting rights in the General Assembly, any interested individuals or organisations (including without limitation representatives of Signatories, user organisations, consumer protection bodies, civil rights groups, industry associations, government bodies or agencies, supervisory authorities, academia, or consultancy organisations) may apply for a membership in the General Assembly as Supporter. Signatories may not apply for Supporter Status.

All Supporters will be required to pay the annual Supporter membership fee, as set out by the General Assembly. Supporter status is automatically renewed for another year unless the Supporter does not express its request of termination 3 (three) months prior to the end of their Supporter membership term. Supporters shall be published on the Code website and publicly declare their support to the principles of the Code.

7.1.3.2 Licensor

Separately and without obtaining voting rights in the General Assembly, any interested individuals or organisations (including without limitation representatives of Signatories, user organisations, consumer protection bodies, civil rights groups, industry associations, government bodies or agencies, supervisory authorities, academia, or consultancy organisations) may apply for a membership in the General Assembly as Licensor. Signatories may not apply for Licensor Status.

Licensors shall pay the annual Licensor fees; Licensors shall be entitled, subject to a separate licence agreement, to utilize the Code in their own Code of Conduct initiatives.

Licensor status is automatically renewed for another year unless the Licensor or the General Assembly does not express its request of termination 3 (three) months prior to the end of their Licensor membership term. Licensors shall be published on the Code website and publicly declare their support to the principles of the Code.

7.1.4 Secretariat

The Secretariat performs the functions as assigned by this Code and rules of procedure, or any subordinate agreements. Besides, following functions shall be performed:

- Promote the Code in Member States;
- Maintain the Code website;
- Perform other related functions at the request of the Steering Board or the General Assembly.

Unless decided differently by the General Assembly, GDD and Bitkom shall be considered the Secretariat.

7.2 Code and guidelines

A regular review of the Code and the Code guidelines to reflect legal, technological or operational changes and Good Practices, as well as experiences in the practical operation and application of the Code, shall take place when appropriate, and in any event at least every three years. Good practice initiatives shall be integrated and referenced where appropriate.

An additional review of the Code and the guidelines can be initiated at the request of two members of the Steering Board or the Monitoring Body.

The Steering Board may appoint a drafting team to conduct the review.

The General Assembly shall submit the revised Code for endorsement in accordance with Art. 40 GDPR, whenever there has been a change to the Sections 2 to 4 and 6of this Code. Comments from the supervisory authorities and the European Data Protection Board should be incorporated as appropriate, approved by the General Assembly, and published. To the extent the Code allows for further particularisation by guidelines or supporting documents, such guidelines and supporting documents must not undermine or materially affect neither the provisions and safeguards of the Code, nor the powers of the Monitoring Body.

7.3 Finances

7.3.1 General

The costs for the Secretariat (see 7.1.4), if applicable, and the Monitoring Body (see S6.2) should be covered by fees raised by its Members and Supporters.

All fees are publicly available.

7.3.2 Secretariat

The General Assembly shall have the power to decide on the adequate share of the membership fees to cover the Secretariat administration costs.

7.3.3 Monitoring Body

The Monitoring Body shall have the power to request fees for each declaration of adherence regarding a pseudonymisation process or any other activity within the performance of its function under Art. 41 GDPR. Those fees apply regardless of the outcome of the declaration of adherence.

7.3.4 Complaints

Complaints may be subject to fees, which shall be cost-based and approved by the General Assembly. Detailed provisions are governed in Section 6.8.3 of the Code.