Deliverable 4.9.3.a

Legal Approach to Enable Data Sharing

Funded by

Federal Ministry of Research, Technology and Space

Funded by the European Union

NextGenerationEU

https://anomed.de

UAP	4.9.3
Editorial Deadline	July 2025
Version	1.0
Status	Final
Distribution	PU
Lead Contributors (© by affiliation)	Bud P. Bruegger (ULD)
Additional Contributors (© by affiliation)	Harald Zwingelberg (ULD)
Reviewers	Niklas Zapatka (UHH-SVS)
License	CC-BY 4.0

Table of Contents

1 Acknowledgements

Early ideas on this topic were developed in the PANELFIT[1] project and documented in an internal-only discussion paper called "Transferrable Consent". PANELFIT has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

The ideas were then further developed in the TRAPEZE project, but did not find their way into actual project deliverables or other forms of publication. The TRAPEZE project received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883464.

2 Introduction

This section provides the necessary context to the work that was conducted under the according project task.

In the context of European data spaces, the planned objective of this task was to construct solutions mainly based on legal constructions to enable data flows that are representative for data sharing for secondary uses.

Two factors required a slight re-orientation of the planned work:

- Since the time of drafting the AnoMed project proposal, the EHDS has evolved and been clarified such that in its field of applicability, it already provides the sought concepts and thus already solves the perceived problems. The solution provided by the EHDS is mostly applicable to public bodies who share their data; the question how private actors can share data in areas that are not covered by the EHDS or other EU data spaces remains unanswered, however. For this reason, the focus of the reported work was on this "gap". It remains relevant since it is for example applicable to data markets or commons.
- The originally planned work was targeted to be executed by a legal researcher. The actual staffing situation rendered this impossible but a researcher with a technical background was available. Consequently, the work was reoriented to take a more technical direction with a more thorough analysis of the form that the proposed concepts need to have in order to create actual practical impact.

3 Main Results

The reported work led to two major results that are describe in detail in Sections 4 and 5, respectively.

[1] Link here

The first result are concepts that permit the sharing of data for secondary use outside of EU data spaces in a GDPR-compliant manner. It represents the actual objective of the work.

While working on this objective, the question repeatedly came up on how a resulting concept can be presented in order to have an actual impact in practice. The danger that the authors attempted to avert was to write "yet another project report that is not read by anyone and whose main impact is to collect dust on some shelf". This meta-discussion led the authors to experiment with the format in which to write the resulting concepts. In particular, how could the result be made accessible to implementers who lack a high level of legal data protection expertise? Also, how can a project result be made easy to reuse. This line of thought led to the GDPR concepts of "policy" (see Art. 24(2) GDPR) and Code of Conduct (see Art. 40 GDPR). Thinking in this direction, substantial effort went into experimenting with a writing format and structure that is suitable for this purposes. This experimentation is shown in the resulting section 4. The experimentation shows for example in the statement of functional requirements in the description of necessary technical and organizational measures.

To capture this more methodological experience for future research work and for consideration by others, the experience was documented in a draft publication (see section 5). In the hope that it has a wider relevance for the operationalization of data protection, at the time of writing, the authors seek a suitable publisher (such as a journal or a European-level data protection body).

4 Rendering data sharing in the private sector possible

This section represents the first major result of the reported work. In particular, it attempts to describe a concept, how personal data can be shared for secondary use in a GDPR-compliant manner.

4.1 Main risk: "data ownership"

In many discussions[2] on data sharing by private actors the concept of "data ownership" assumes a significant role. In this concept, data holders "own" the personal data that they have legally collected. The collected data is often seen as a valuable asset. This is for example evident in the expression that "data are the new oil".

The data ownership point of view stands in a certain conflict with the point of view that data protection is a fundamental right (see Art. 8 of the European Charter of Fundamental Rights) that the basis for the GDPR. In particular, data subjects are a party with rights in any processing of their data. This includes secondary uses. These rights, since fundamental, also cannot just be "sold", and thus relinquished, as the concept of "ownership" would imply.

The concept of data ownership is highly attractive in discussions since:

- Due to its **analogy to** society's management of **material goods**, it is **easy to understand**. This stands in contrast to fundamental rights and the GDPR that lack a well-known analogy and, for most players, are far more difficult to understand.
- How to implement data sharing (for example, in a data market) based on ownership is well understood and therefore "straight forward". In contrast, the requirements by the GDPR are less understood and often seen as an excessive complication that prevents data sharing and its potential benefits to society.

[2] Namely, the discussions that the authors participated in as part of previous projects.

In this context, the concept described in section 4 tries to propose a solution how data sharing is possible in compliance with the GDPR and without the use of "data ownership". The focus on the work was to find ways to avoid disenfranchising data subjects during secondary use.

4.2 Approach

There are many possible approaches of how to structure a data protection analysis how to enable secondary use. The considerable meta-thought that went into this question resulted in three guiding principles:

(i) Maximize structure and consistent, systematic treatment of similar concerns.

(ii) Attempt to reach tangible, concrete statements that leave little room for interpretation.

(iii) Model the structure closely to the structure that is implied by the GDPR for compliance.

(i) The attempt of applying these principles resulted in a focus on individual technical or organizational mitigation measures (TOMs). Systematically, they follow the very same structure.

(ii) To reach a high level of concreteness, for each discussed TOM, functional requirements are stated. These can be understood by readers who lack profound data protection knowledge or are versed in the interpretation of the legal text of the GDPR.

(iii) Since the main objective of the developed sharing concept is to reach GDPR-compliance, the structure inherent in the GDPR was identified and applied. In particular, Art. 24(1) which describes the main obligation of controllers states that "the controller shall implement **appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation". In other words, compliance is achieved though the implementation of TOMs. Based on this inherent structure, the proposed concept uses TOMs as primary structure element.

At least for processing activities with high risk, Art. 35 GDPR further describes the general process to reach compliance. In particular, Art. 35(7)(c) GDPR states that risks to the rights and freedoms of data subjects need to be assessed. Art. 35(7)(d) further that the role of TOMs in reaching compliance is to address the identified risks. Consequently, the chosen structure explicitly states the risk (called "shortcomings") that is being mitigated by each given TOM.

This approach is visualized in Figure 1. After a general description of the addressed problem (i.e., secondary use and sharing of personal data), a first implementation solution is described. It represents that most straightforward implementation option that is likely the first consideration of potential controllers. This implementation solution is considered the baseline that is then continuously refined. In particular, in a given solution, compliance risks (called "shortcomings") and a TOM is proposed that is suited to appropriately mitigate this risk. This results in an improved implementation that is then the input to a consecutive improvement step. The continuous refinement ends when no more compliance-risks can be identified and the resulting refined solution can therefore be considered as being compliant.

Note that the proposed solution is by no means guaranteed to be fully GDPR compliant. In particular, such compliance can only be asserted by the competent supervisory authority or a court. The proposed solution may well be subject to unidentified risks and the proposed mitigation measures are not guaranteed to be appropriate to sufficiently mitigate the identified risk.

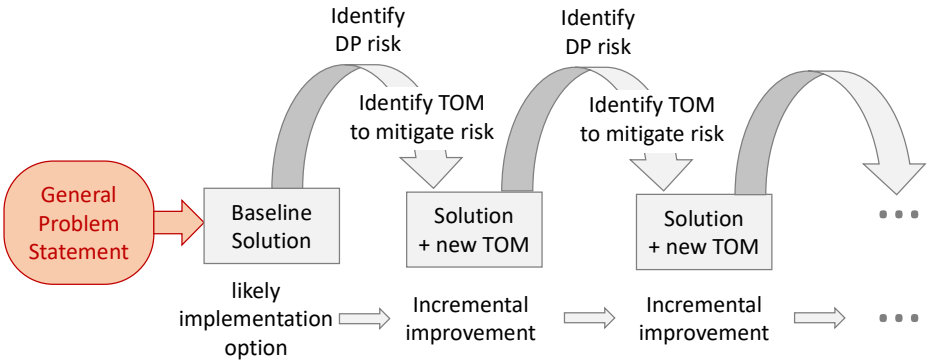

Figure 1: Approach taken to develop a concept for secondary use of personal data.

4.3 Outline of Section 4

The remainder of Section 4 starts with describing a generic **processing scenario** that is the object of study of this paper. For this scenario, a **baseline solution** approach is then described and evaluated. This evaluation identifies the main data protection risks[3] of the processing. In addition, a hypothesis on how the situation is perceived by data subjects is presented. Following an approach of data protection by design (Art. 25(1) GDPR), technical and organizational measures (TOMs) are proposed that mitigate certain identified risks. The effect of each proposed TOM is then evaluated. Where a TOM introduces shortcomings or risks of its own, additional TOMs are proposed as mitigation measures.

4.4 Processing Scenario

This section describes a processing scenario, i.e., a category of processing activities, that is the object of study. To foster clear and unambiguous analysis, it proposes a terminology to denote the various entities of the scenario. It then describes some characteristics of communication in the scenario. It summarizes the situation in a section on the scope of processing.

4.4.1 Description

The processing scenario that is the object of discussion is visualized in Figure 2.

[3] The term "risk" here refers to the danger that data protection principles and are insufficiently implemented.

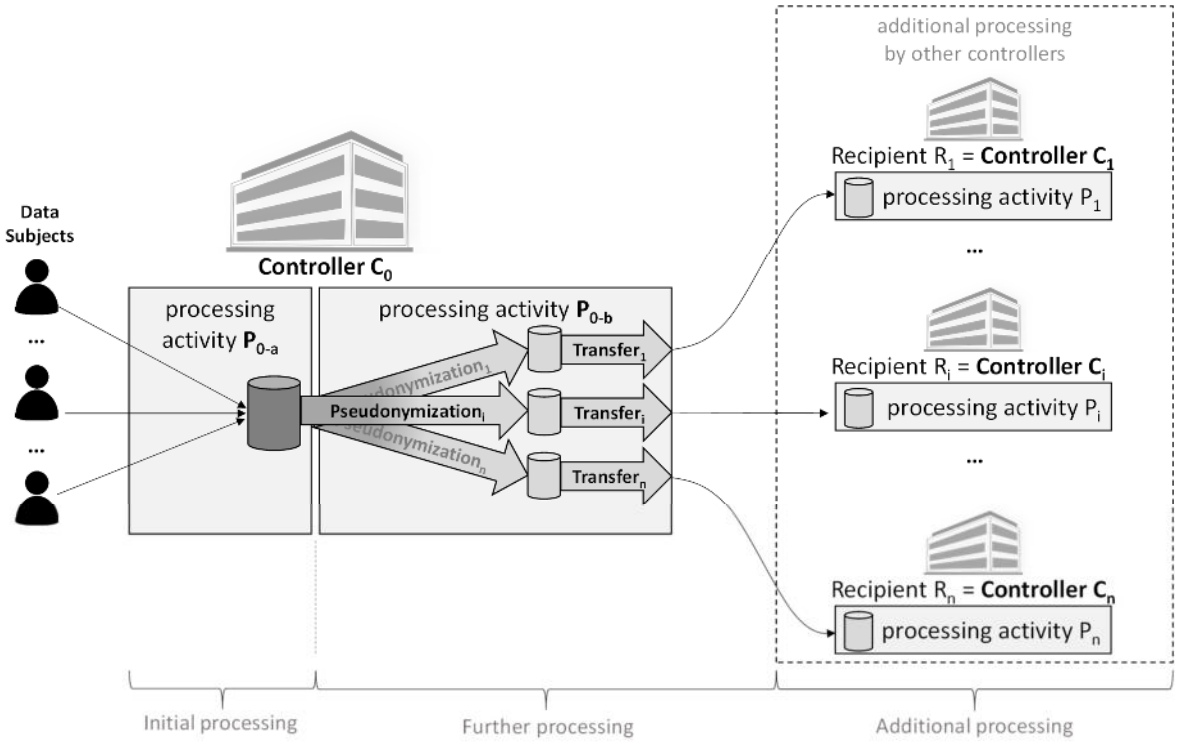

Figure 2: Scenario of processing activities.

The following describes the figure in more detail:

- The **Controller C_0** executes an **initial processing activity P_{0-a}** for which the personal data was collected. This processing activity is mostly out of scope of the present discussion since the focus is on further and additional processing of the collected personal data that goes beyond the initial processing.
- The **further processing** of the initially collected personal data is that processing in the scenario by the controller C_0 that is not necessary for the purposes of the initial processing. Namely, the **Controller C_0** first needs to **transfer** the data to the recipients of the pseudonymized personal data. According to Art. 4(2) GDPR, "disclosure by transmission, dissemination or otherwise making available" constitutes "processing". Since it is not part of the initial processing P_{0-a} but belongs to the further processing, it is shown here as a separate **processing activity P_{0-b}**. Usually, in addition to the actual **data transfer to recipients**, **P_{0-b}** also includes an optional processing step of ***pseudonymization***. Where directly identifying data elements are unnecessary for the various purposes of further processing, pseudonymization is a mandatory processing step according to Art. 5(1)(c) "data minimization" and 5(1)(e) "storage limitation".
- Once received that personal data from controller C_0, the n **controllers C_1** through **C_n** operate their own **processing activities P_1** through **P_n**. Evidently, each controller C_i is **also a third party recipient** of the personal data initially collected by C_0. The same entity can thus be identified as C_i or **R_i**, depending on whether the focus is on their role as a controller of further processing or as a recipient of personal data.

4.4.2 Terminology specific to the scenario

To facilitate the analysis of this paper, it is useful to define some terms to more easily refer to entities of Figure 2. This includes the following terms:

Initial controller	The controller $\mathbf{C_0}$ responsible for the initial processing $\mathbf{P_{0\text{-}a}}$ is called ***initial controller.***
Initial (original) **processing**	The processing activity $P_{0\text{-}a}$ by controller C_0 is called ***initial processing***. *Original processing* is sometimes used as a synonym.
Initial (original) **purposes**	The purposes of the initial processing are called ***initial*** or *original* ***purposes***.
Initial (original) **data**	The personal data that was collected by controller C_0 for the initial processing is called ***initial*** or *original* ***data.***
Pseudonymization and **Transfer**	The processing activity $P_{0\text{-}b}$ is called ***pseudonymization and transfer*** or sometimes simply ***transfer.*** It constitutes *further processing* by the initial controller C_0 that is not required for the initial purposes of the initial processing.
Pseudonymized data	The personal data that are actually transferred to recipients are called ***pseudonymized data***. They are pseudonymized, as evident from the term. The pseudonymization may be different for different recipients, such that a linking of data held by different recipients is rendered impossible. In addition to pseudonymization, the data may also be a subset of the original data. The subset may be different for different recipients.
Other controller	The controllers C_1 through C_n who receive personal data from the initial controller C_0 and process them in the processing activities P_1 through P_n, respectively, are called ***other controllers***. Other controllers are also (third party) recipients of the initial data.
Additional processing	The processing activities P_i of another controller C_i is called ***additional processing***.
Other purposes	The purposes of the additional processing by other controllers are called ***other purposes***.

4.4.3 Communication in the Processing Scenario

As a direct effect of pseudonymization, other controllers are unable to attribute the received data to an identified or identifiable person. This has the consequence that other controllers are unable to establish communications with data subjects. This is evident when considering that any address routinely used in communications (such as e-mail address, street address, or telephone number) are typically eliminated by pseudonymization.

This means that controllers can initiate a communication with data subjects only if the technical design of the overall processing foresees a specific architectural component that enables such communications.

The ability of data subjects to initiate communications with other controllers is unaffected by pseudonymization and possible whenever data subjects know the identity (and contact information) of other controllers.

4.4.4 Scope of processing

The following gives a brief overview of the above processing scenario. It attempts to specify the scope of processing, as required in a code of conduct[4].

processing operations	Reuse of Personal Data in Additional Processing Activities by Third Parties

[4] EDPB Guidelines 1/2019 on Codes of Conduct, paragraph 23.

personal data covered	The scenario is generic and imposes no restriction on the personal data used.
categories of controllers	The scenario is generic and is applicable to a wide range of industries and controller.

The **processing issues addressed** are transparency and implementation of data subject rights. They are illustrated in more detail in the sequel of this paper.

The same goes for the **practical solutions** which attempt to address the issues.

4.5 Baseline Solution Approach

The following describes a solution that is used as a baseline. It is possibly the most straightforward approach that requires the least conformance effort from the various controllers, and is likely commonly used in practice. As a baseline, this solution approach serves to point out risks and is the basis for a hypothesis about how data subjects experience the situation.

4.5.1 Description

Like for all processing operations, the initial controller C_0 needs a legal basis for pseudonymization and transfer. In this scenario and across all solution options, it is assumed that this legal basis is consent (i.e., Art. 6(1)(a) GDPR).

Where a data subject consented to pseudonymization and transfer by the initial controller C_0, the recipients R_1 through R_n receive a pseudonymized subset of personal data. The recipients are controllers in their own right and therefore synonymously called C_1 through C_n. These controllers are completely free in determining the purposes and means of their processing of the received data.

The baseline solution approach assumes that controllers C_1 through C_n choose **legitimate interest** (according to **Art. 6(1)(f) GDPR**) as **legal basis** for their respective processing activities.

Since these controllers have not obtained the data from data subjects, Art. 14 GDPR regulates how data subjects have to be informed about the additional processing. Since the pseudonymization prevents the possibility that controllers push the necessary information to data subjects (see above), **Art. 14(5)(b) GDPR** applies. The controllers therefore informs about their processing "by making the necessary information publicly available"[5]. This is typically done by presenting the information on (part of) a web page on the controllers web site.

4.5.2 Evaluation

The baseline solution has two main issues:

- **Transparency** (see Art. 5(1)(a) GDPR) and
- **Data Subject Rights** (see Chapter III GDPR).

The fact that the controllers of additional processing are unable to contact data subjects and thus send them the information required by Art. 14 GDPR gravely hinders transparency for data subjects. Even if controllers publish adequate information about their processing in a prominent place[6] within their web presence, it is likely that many of the concerned data subjects never learn about the processing of their personal data. Transparency is even worse if controllers of additional processing

[5] This is the wording of Art. 14(5)(b).

[6] A prominent place would for example be a well visible link on their home page.

put the necessary information in a less prominent position or even attempt to hide it “in the depth” of their web presence.

In order to invoke their rights, data subjects need to know the identity of the controllers and how to contact them. Due to a lack of transparency, this prerequisite is often not in place. Consequently, data subjects are deprived of their rights.

A secondary issue with the baseline solution approach may be for which purposes the collected personal data are used. Data subjects may hold the **reasonable expectation** that their data are not used for completely different (and thus incompatible) **purposes** than the known ones of the initial processing.

Since the controllers of the additional processing are completely free in determining the purposes of their processing, there are no mechanisms in place to limit or restrict the purposes pursued by the recipients of the data.

Even if the consent for the data transfer was to specify purposes for the processing by third party recipients, no mechanism is in place to legally bind recipients to honor such a limitation. Similarly, enumerating the actual recipients or specifying the category of recipients in the consent to the data transfer fails to effectively limit the possible purposes. This becomes evident when considering that a given recipient could also pursue atypical purposes.

4.5.3 Possible Perception by Data Subjects

To data subjects, it may seem that with the consent to the data transfer by the initial controller, they also consented to all the additional processing by other controllers. They may not understand the intricacies that the legal basis for the transfer of data by the initial controller is distinct from the legal basis that recipients of the data need for their processing.

If the consent for data transfer really provided a legal basis for the processing by recipients, its underlying would fall far short of the concept of consent in the GDPR. In particular, it would at least have the following shortcomings:

- The purposes of processing by the recipients are undefined; and
- such “consent” cannot be withdrawn.

These thoughts about the possible perception of the consent to transfer by data subjects may indicate that data subjects would expect more control in the dialog that collects consent to transfer.

This is also understandable from the point of view that this consent dialog is the last point in time before the personal data leave the domain of control by data subjects. In the described baseline solution, data subjects may get the impression that once the consent for transfer was given, the personal data disappear in a domain of darkness that is void of any scrutiny.

Likely, beyond just bringing more light into that domain of darkness, data subject would want to exercise more control over future processing at the last point in time where they are actively involved.

4.6 Technical and Organizational Measures (TOMs)

Following the approach of data protection by design, this section describes technical and organizational measures suited to mitigate the risks that were identified in the baseline solution. Some also aim at bringing the user experience closer to the expectations of data subjects. Here, particularly an improved control at the last time of interaction is of interest.

The discussion of each TOM starts with a statement about the shortcomings it addresses, describes the actual measure, and then evaluates the effectiveness of the measure. The evaluation may also identify shortcomings introduced by the measure itself.

4.6.1 TOM1: transparency dashboard

4.6.1.1 Addressed shortcomings

This TOM addresses the shortcoming of transparency, namely that it is impossible for other controllers of additional processing to find an adequate communication channel through which to inform data subjects about the processing (as required by Art. 14 GDPR).

4.6.1.2 Description

This TOM consists of a "transparency dashboard" that is operated by the initial controller. Prior to transferring data to a given recipient R_i, the initial controller obtains the **information according to Art. 14 GDPR from the recipient**. This information is then "loaded" into the dashboard and made available to all data subject concerned by the data transfer and thus the additional processing. These data subject are those who consented to the data transfer.

Functional Requirements:

- The transparency dashboard presents a page to affected data subjects showing the information on additional processing according to Art. 14 GDPR as received from the data recipient.

The transparency dashboard also provides data subjects with an **overview page** where all (still active) recipients of a data subject's data are listed and from where the data subject can navigate to the more detailed information about additional processing by a selected recipient. The list of recipients is of particular importance in the case where data subjects consent to the transfer of data to whole categories of recipients without having access to a concrete enumeration of recipients.

Functional Requirements:

- The transparency dashboard presents an overview page to affected data subjects that lists all (still active) recipients of their data.
- The list items can be used to navigate to more detailed information about the processing by a given recipient.

The Art. 14 GDPR information of recipients is visible as long as the additional processing by the recipient takes place. This was referred to as "still active" above. To be able to show pertinent information to data subjects, the primary controller also needs to store the data about consent to the data transfer for that period of time.

4.6.1.3 Evaluation

A transparency dashboard, compared to Art. 14 GDPR information being served somewhere on the recipients' web sites, renders it **much easier for data subjects to be informed** that certain additional processing takes place and what it consists of. Moreover, the overview page of the transparency dashboard provided data subjects with a **single point of access** to see who has received their data and for what purposes they are processed.

Since Art. 14(1)(a) and (b) also list the necessary contact details that are necessary for **data subject**s to be able to exercise their **rights**. The implementation of data subject rights by recipient is still

hampered by the fact that they are **unable to map the identity of data subjects to the pseudonym** that was created by the initial controller.

In absence of additional TOMs, the Art. 14 GDPR information provided by different recipients can vary widely in format and style. This **absence of a common look and feel** renders it more difficult for data subjects to find and access the information sought after.

4.6.2 TOM2: Standardized Presentation of Art. 14 GDPR Information

4.6.2.1 Evaluation

The common look and feel of Art. 14 GDPR information renders it much easier for data subjects to understand how their data is processed.

4.6.2.2 Addressed shortcomings

This TOM addresses the shortcoming that Art. 14 GDPR information provided by different recipients could be presented completely different and thus require an increased effort by data subjects to understand what their data are used for.

4.6.2.3 Description

The TOM addresses how the Art. 14 GDPR data is provided by recipients and how it is presented to data subjects in the transparency dashboard.

Recipients of data need to provide their Art. 14 GDPR information in a **standardized language** that uses a **standardized vocabulary**. Such standardization has, for example, been pioneered by the SPECIAL and TRAPEZE projects (https://specialprivacy.ercim.eu/, https://trapeze-project.eu/). They have both collaborated within the W3C Data Privacy Vocabulary Community Group (https://www.w3.org/community/dpvcg) to create a standard vocabulary. These projects use this vocabulary in their policy languages.

Functional Requirements:

- A formal language and vocabulary in which recipients need to provide Art. 14 GDPR information is defined and documented.
- The transparency dashboard uses a common look and feel across recipients to present Art. 14 GDPR information to data subjects.
- Optionally, the transparency dashboard can present a possibly more detailed free text version of Art. 14 GDPR information on request by data subjects.

4.6.3 TOM3: Consent Dialog for Data Transfer

4.6.3.1 Addressed need

The transfer (processing activity $P_{0\text{-}b}$ in Figure 1) requires consent as a legal basis.

4.6.3.2 Description

The initial controller presents data subjects with a consent request to establish a legal basis for the transfer of data to the recipients.

In its guidelines on consent, the EDBP states the following[7]:

[7] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, page 15, paragraph 64.

"Therefore, the EDPB is of the opinion that at least the following information is required for obtaining valid consent:

i. the controller's identity,
ii. the purpose of each of the processing operations for which consent is sought,
iii. what (type of) data will be collected and used,
iv. the existence of the right to withdraw consent,
v. information about the use of the data for automated decision-making in accordance with Article 22 (2)(c)36 where relevant, and
vi. on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46."

Applied to the consent dialog for data transfer, this should be interpreted as follows:

i. The controller of the data transfer is the initial controller; the dialog must therefore specify the initial controller's identity.
ii. The purpose is to transfer the data to certain recipients. It can be argued that the purpose is insufficiently specified unless it actually specifies the recipients.
iii. The data to be transferred is a pseudonymized version of a subset of the data collected for the initial processing activity $P_{0\text{-}a}$. What that subset contains and the fact of the pseudonymization should be specified in the consent dialog.
iv. The consent to the data transfer constitutes a legal basis for the transfer. It is distinct from the legal basis of additional processing by the recipients. According to Art. 7(3), second sentence, "The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal." Therefore, the withdrawal of consent is only possible before the transfer has taken place. Thereafter, withdrawal of consent has no effect and, arguably, is no longer possible. The consent dialog should create realistic expectations for data subjects as for the possibility and effect of withdrawing consent.
v. Data transfer is not considered to be "automated decision-making" and the consent dialog can therefore refrain to inform about it.
vi. The consent dialog has to inform about the mentioned risks for the case where recipients are located in third countries.

Functional Requirements:

- The dialog requesting the consent to data transfer must contain all the information elements as discussed above.

4.6.3.3 Evaluation

The evaluation addresses two aspects relative to the informedness of consent decisions:

i. Specification of a multitude of recipients and human cognitive limitations;
ii. Need to know the purposes of the additional processing by recipients.

(i) A first aspect of evaluation focuses on the specification of the recipients that is part of the purpose specification. In particular, two aspects are of interest here, namely how to handle a potentially large number of recipients.

When dealing with more than a handful of recipients, data subjects' cognitive limitations are likely to impede an informed decision about the consent request. In particular, it was found that only seven

plus minus two different entities can be grasped by humans[8]. When the number of recipients exceeds this number, data subjects are typically unable to take in the whole list. More likely, data subjects look at the first and the last few listed recipients as a decision basis. Possibly, some random samples in between are also looked at. This invites the risk of "hiding" undesirable recipients within a large number of acceptable ones.

(ii) A second aspect of evaluation focuses on whether data subjects can make informed decisions in absence of knowing the **purposes of additional processing** by recipients. In the baseline solution approach, recipients use legitimate interest (Art. 6(1)(f) GDPR) as a legal basis for their processing. Recipients are completely free in determining the processes of their processing activities. The present TOM fails to inform data subjects about the purposes of secondary processing.

It can be argued that knowing the identity of recipients is an insufficient basis for making an informed consent decision. The identity of controllers may, to a certain degree, inform about how trustworthy they are to data subjects. Other factors may be relevant for consent decisions too, however. For example, it may be relevant for data subjects how well a recipient's field of activity fits with declared purposes: A renowned research institution may well be trusted to receive personal data for research purposes while an organization selling market surveys may not. Also, data subjects may judge the use of their data at hand for certain purposes less sensitive than others. Consequently, consent decisions for data transfer are better informed if the purposes pursued by recipients are declared as part of the consent dialog.

As stated in section 4.5.3 above, data subjects may perceive the consent to data transfer dialog as actually providing a legal basis to recipients for their processing. If this was indeed the case, a specification of the purposes pursued by recipients would be a mandatory element of the consent request. This further underlines the necessity of specifying the purposes of additional processing in the consent request dialog and the need to find a measure with which the initial controller can legally restrict recipients to the purposes specified in the consent request dialog.

4.6.4 TOM4: Use of Categories of Recipients in Consent to Transfer Dialog

4.6.4.1 Addressed shortcomings

This TOM addresses the cognitive limitation of data subject that impede informed consent decisions in presence of large numbers of recipients.

4.6.4.2 Description

The dialog requesting consent for data transfer uses short categories of recipients instead of much longer enumerations of recipients.

Functional Requirements:
• The dialog requesting the consent to data transfer must contain all the information elements as discussed above.

4.6.4.3 Evaluation

Categories of recipients are more abstract than enumerations. They delegate the responsibility of determining membership of a concrete recipient in the category to the initial controller. An additional TOM is necessary to make this delegated membership decision subject to scrutiny.

[8] Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review, 63*(2), 81–97. https://doi.org/10.1037/h0043158

An enumeration of recipients cannot be changed at a later point in time without changing the subject of consent. In contrast, if a decision whether a given recipient belongs to the consented category is made at a later point in time, this leaves the subject of consent completely unaffected.

This fact makes it possible to add recipients at a later point in time. Evidently, at any point in time must it still be possible to expand categories of recipients into enumerations.

4.6.5 TOM5: Possibility to expand categories of recipients into enumerations of recipients

4.6.5.1 Addressed shortcomings

The previous TOMs lack scrutiny of the decision by the initial controller of whether a given recipient belongs to a given category.

4.6.5.2 Description

Such scrutiny is enabled by giving data subjects the possibility to expand categories of recipients into enumerations.

Functional Requirements:

- Data subjects must have the possibility to expand categories of recipient used in the consent to transfer dialog into enumerations. This must be possible at any point in time.

4.6.5.3 Evaluation

This TOM is effective in addressing the shortcoming.

Since in the given scenario (see Figure 2 above), recipients are already enumerated on the overview page of the transparency dashboard (see TOM 1 above), the latter can be considered a valid implementation of the present TOM.

The overview page of the transparency dashboard also satisfies the requirement that data subjects must be enabled to expand categories to enumerations at any point of time so all information is nevertheless available.

4.6.6 TOM6: Contract to Limit Purposes

4.6.6.1 Addressed shortcomings

The evaluation of TOM3 identified the need of specifying the purposes pursued by recipients in the consent to data transfer. A TOM is required to legally restrict recipients to the purposes specified in their consent request. This can also be seen as giving the data subject control over the purposes pursued by recipients.

4.6.6.2 Description

The following assumes that the consent request dialog for transferring the data explicitly states the purposes that can be pursued by recipients. Since this was not already part of TOM3, it is stated here as monitorable functional requirement.

Functional Requirements: (addition to TOM3)

- The dialog requesting the consent to data transfer must specify the possible purposes that can be pursued by recipients.

Since the consent to data transfer is granted to the initial controller, it is not legally binding for recipients. Therefore, a special legal instrument is necessary. This could be a contractual agreement

between the primary controller and the recipient that restricts the recipients in their freedom of determining purposes of processing to those purposes specified in the consent to transfer.

Such as contract may have similarities with contracts according to Art. 28(3) in which controllers express mandates to processors.

Functional Requirements:
• A contract must be established between the initial controller and recipients that legally restricts the recipient in the possible purposes of their processing in accordance with the purposes stated in the consent to data transfer.

4.6.6.3 Evaluation

Collecting consent from a data subjects on behalf of other controllers will require legal construction to match the legal requirements. Given that, the necessary information about the intended processing has been provided the declaration of consent needs to be expressed in a way that is legally relevant between data subject and recipient. The initial controller may act as an agent on behalf of the recipient or provide pre-issued declarations of the recipient and thus have the role of a communication messenger. A contract between controller and recipient needs to establish these roles, define reciprocal responsibilities, e.g. that a withdrawal of consent or objection addressed to the received by the initial controller on behalf of the recipient has to be complied with by the latter. It should also establish ways allowing data subjects and recipients to interact independently of the initial controller e.g. to execute data subject rights or declare an objection.

Such a contract may only be binding for actual (direct) recipients but do not extend to indirect recipients who obtain the data form direct recipients who disclose the data further.

Certain highly unwanted purposes, such as the (re-) identification of pseudonymous personal data, may merit explicit treatment in the contract.

4.6.7 TOM7: Further disclosure and Re-Identification in Contracts with Recipients

4.6.7.1 Addressed shortcomings

This TOM is designed to close loopholes of further disclosure of personal data by recipients as well as explicitly excluding particularly undesirable purposes.

4.6.7.2 Description

The contract between initial controller and recipients shall regulate redistribution of the data by recipients. In particular, it shall contain one of the following options:

- Recipients must refrain from any re-distribution of the received data, including disclosure by publishing.
- Alternatively, if re-distribution is permitted, recipients are obliged to pass on the limitation of possible purposes of processing.

Functional requirements:
• The contract between initial controller and a recipient regulates whether re-distribution is allowed and under what conditions.

Certain particularly undesirable purposes merit additional measures to be rendered impossible. The contract between initial controller and recipients shall therefore oblige the recipient to implement adequate technical and organizational measures to render the use of the received data for certain purposes impossible. This is the case for example regarding the possibility of re-identification of the

received pseudonymous data. Note that Art. 4(5) GDPR on pseudonymization includes the following wording: "… 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…". Evidently, pseudonymization does not only require the observations of these obligations by the initial controller. Much rather, also recipients must ensure that the pseudonymous data is kept separate from additional information that is suited to re-identify data subjects. Recipient must also implement suitable technical organizational measures to prevent any kind of re-identification. This may for example include awareness building among the recipient's employees or inclusion of adequate rules in codes of conduct for employees. When a recipient uses processors, these obligations should be contractually passed on.

Functional Requirements:

- The contractual agreement between the initial controller and recipients shall pass on obligations to implement suitable technical and organizational measures that are required for pseudonymization.
- Such obligations must also be passed on to possible processors.
- Where the initial controller permits re-distribution, these obligations must also be passed on to parties to whom the data is disclosed.

4.6.7.3 Evaluation

This measure seems effective in mitigating the addressed shortcomings.

4.6.8 TOM8: Let users choose purposes (like consent)

4.6.8.1 Addressed shortcomings

While legally, a consent to the transfer of data is not a consent for the processing by recipients, data subjects often perceive that this is the case. It is therefore fair to fulfill all the requirements that would be present if it actually was a consent to the recipients' processing.

Where consent is required in exchange for access to services or the performance of a contract it becomes questionable if the consent was provided freely, Art. 7(4) GDPR. Even more so the processing by yet further parties, the recipients, becomes questionable. Where a dialogue asking for consent to share data with recipients provides not only a means to choose potential recipients but also the purposes the recipients intend to pursue, the more fine grained means for selection partly re-empowers data subjects in their freedom to decide.

4.6.8.2 Description

The present TOM consists in fulfilling all requirements for a fictive consent to the processing by recipients also in the consent to the transfer of data.

A prominent example for this is that purposes of processing should not be bundles into an all or nothing package deal. Therefore, if the consent dialog specifies multiple independent purposes for the processing by recipients, these should be separated into distinct consent decisions. For example, the purposes of "conducting scientific research" and "conducting market research" should not be bundled but require distinct consent decisions from data subjects.

Functional Requirements:

- In the dialog requesting consent to transfer, separate consent decisions are offered to data subjects for unrelated purposes of processing by recipients.

4.6.8.3 Evaluation

This TOM is effective to improve fairness and give increased control over processing of personal data to data subjects.

4.6.9 TOM9: Data Subject Rights Dashboard

4.6.9.1 Addressed shortcomings

While the transparency dashboard (TOM1) guarantees that data subjects have access to contact information of recipients (i.e., controllers of additional processing), pseudonymization executed by the initial controller can make it impossible for recipients to identify which data belong to given data subjects who invoke their rights.

4.6.9.2 Description

The initial controller can keep the additional information necessary to convert a data subject's (potentially full) identity as known to the initial controller to a pseudonym known to a recipient.

The data subject rights dashboard is operated by the initial controller and consists in a messaging system, where data subjects can send messages to recipients. It automatically converts data subject's identity used to access the dashboard to pseudonyms known to the recipient. The data subject rights dashboard can be integrated with the transparency dashboard into a single "data protection dashboard".

Functional Requirements:

- The initial controller operates a data subject rights dashboard that permits data subjects to initiate and conduct conversations with recipients of data.
- The dashboard translates the identity seen by the initial controller to a pseudonym known to the recipient.
- The contractual agreement between initial controller and recipient mandates that recipients monitor their "inboxes" and process data subject right invocations through this communications channel.

4.6.9.3 Evaluation

The transparency dashboard requires only a one-time communication (of Art. 14 GDPR information) from the recipient to the initial controller. The data subject rights dashboard, in contrast, requires an increased effort/commitment from both the initial controller (who operates this dashboard) and recipients who commit to process any requests made by data subjects through the dashboard. Whether this effort is necessary must be determined based on the concrete processing activity.

In the case that the effort is justified and a data subject rights dashboard is operated, it empowers data subjects to, "for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification" (see second sentence of Art. 11(2) GDPR).

5 Meta Discussion: Generalization of the experimentation on how to reach impact

5.1 Introduction

The present essay addresses the question of how to best render data protection laws, most notably the GDPR, operational through the issuance of policy instruments such as controller-internal policies, Codes of Conduct, and similar instruments. The essay attempts to make the authors' reasoning behind this question explicit in the hope of triggering a wider discussion of what actions can be taken to promote effective application of the law and to render it easier for practitioners to comply with its requirements. The authors are interested in the meta question of how to transfer data protection expertise to practitioners.

One element of answering this question is to identify impediments to the effective application of the law. To reason about this question, we use a very simple model of how data protection is implemented in practice. The model is shown in Figure 3. It shows that the implementation requires the translation of the abstract requirements of the GDPR into appropriate concrete actions.

Figure 3: Operationalization translates abstract requirements into concrete actions.

In this context, a major impediment is the lack of clarity, how abstract requirements need to be translated into concrete actions. This impediment is further aggravated by the interdisciplinary nature of data protection. Namely, the requirements are typically studied and well-understood by legal professionals, while the concrete actions are to a significant part implemented by technical experts.

We postulate that the operationalization of data protection is synonymous with the ability to translate abstract requirements into concrete actions.

5.2 Instruments of operationalization foreseen in the law

The following discusses instruments designed to support operationalization that are foreseen in the law, primarily in the GDPR but also in regulations pertinent to data spaces.

The GDPR has to apply to arbitrary processing activities and is worded in a technology-neutral manner. This level of generality causes an intrinsically high level of abstraction. Moving towards more concrete statements is often only possible if the generality and possibly scope are narrowed. In particular, for a concrete processing activity, implemented in a concrete technology, and considering only a subset of requirements, it is much easier to reason about concrete actions that are necessary for compliance than would be for the general case.

We call the result of limiting the generality of processing and the requirement under consideration a *concrete case of processing*. For efficiency, we assume that the reasoning of how to implement requirements is the same (or very similar) for whole families of *concrete processing cases*. The term ***concrete family of processing*** captures this situation.

The question arises whether the GDPR foresees means to guide controllers on how to implement its requirements for concrete cases and families of processing. Indeed, the GDPR foresees instruments that aim to provide such guidance:

In its **Art. 24(2)**, the GDPR foresees the instrument of an (controller-internal) ***policy***. While policies with a general scope may exists, we assume that a large part of policies is limited to addressing a concrete case of processing and a subset of compliance requirements. Such policies are typically applicable to a multitude of processing activities of the issuing controller. For example, a controller could write a policy about how to handle pseudonymization of customer data, or how to handle permanent deletion of no longer required data. Similarly, a policy could address the security aspects (i.e., the requirements from Art. 5(1)(f) GDPR) for all database applications with external web interfaces.

In its **Art. 24(3)**, the GDPR gives controllers the option of using ***Codes of Conduct (CoC)***[9]. In essence, they fulfil the same purpose as policies. Namely, they guide controllers on how to implement data protection requirements for a concrete family of processing. What is different compared to a policy is the CoCs' economy of scale. In particular, while a policy applies to a multitude of processing activities of a single controller, a CoC applies to a multitude of processing activities across a multitude of controllers. CoC owners are therefore typically associations of multiple controllers in a single industry (who shares a concrete family of processing), i.e. industry associations (see Art. 40(2) GDPR). Also in contrast to policies, according to Art. 40(5) and (7) GDPR, a CoC has to be approved by the competent Supervisory Authority or the Board prior to use.

Also in its Art. **24(3)**, the GDPR foresees the instrument of ***certification***. For economy of scale, for the present discussion, it is useful to consider the underlying ***conformity assessment scheme***[10] instead of the certificate itself. These schemes describe the precise manner in which certification is conducted for a concrete family of processing. Such schemes thus apply to a multitude of certificates and consequently, a multitude of processing activities of a multitude of controllers. Art. 42(5) states that "A certification […] shall be issued […] **on the basis of criteria** approved by that competent supervisory authority […] or by the Board […]." These *criteria* are part of the underlying *conformity assessment scheme*. In addition, the scheme is also concerned in how exactly these criteria are applied and how the overall process of certification must be conducted. In ISO/IEC 27000 the *criteria* of Art. 42(5) GDPR correspond to the *specified requirements*.

Beyond the GDPR, similar instruments can also be created by other pieces of legislation. For example, in the **proposed EHDS** regulation, **Art. 65(1)(b**) foresees that the *EHDS Board* shall issue "written contributions and to exchange best practices". This renders it likely that the described task also includes the issuance of policy documents. For example, a likely policy could address how to assess "sufficient anonymity" that is a prerequisite for results and outputs to leave the secure processing environment in which they were created[11]. We believe that other data spaces will be very similar in this respect. We therefore assume that data space legislation is likely to create instruments for the operationalization of specific aspects. We call these ***data space policies*** in the sequel.

The above discusses instruments are summarized in Table 1.

Table 1: Overview of relevant operationalization instruments.

	Number of processing activities	**Number of controllers**	**Formal approval** (improved legal certainty)	**Assessment executed by**
No instrument Single processing activity *Art. 24(1) GDPR*	1	1	--	Controller (self-assessment)
Internal policy *Art. 24(2) GDPR*	many	1	--	Controller (self-assessment)

[9] Art. 40(2) GDPR provides examples of possible focus of CoCs. The discussion in this essay considers in particular the one described in point (h) "the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32."

[10] ISO/IEC 17000:2020(E) defines *conformity assessment scheme* (aka *conformity assessment programme*) as the
set of rules and procedures (5.2) that describes the objects of conformity assessment (4.2), identifies the specified requirements (5.1) and provides the methodology for performing conformity assessment (4.1)

[11] For more detail, see Art. 64(11) EHDS Proposal.

Code of Conduct *Art. 40 GDPR*	many	many[12]	By competent supervisory authority or the EDPB *Art. 40(5) GDPR*	Monitoring Body *Art. 41 GDPR*
Conformity assessment scheme that underlies a certification *Art. 42 GDPR*	many	many	By competent supervisory authority or the EDPB *Art. 42(5) GDPR*	Certification Body *Art. 43 GDPR*
Data space policies Data space legislation	many	many [13]	Likely by EDPB or at least by a data space specific body	Data space bodies, such as providers of secure processing environments[14]

The table shows the mentioned instruments in the table rows. In order to capture their inherent economy of scale, it states the number of affected processing activities and controllers. To provide an indication of the degree of confidence and legal certainty[15] created by an instrument, a column indicates whether an instrument is formally approved. Finally, the last column shows the party that uses the instrument for the purpose of assessing the compliance of a given processing activity with the instrument itself.

In the following, the generic term *of **policy instrument*** is used to encompass all instruments listed in the table above.

5.3 The role of policy instruments in the assessment of GDPR-compliance.

This section further analyses the role of policy instruments in the assessment of GDPR-compliance. As a baseline, it first looks at compliance assessment in absence of such policy instruments and then contrasts this with an assessment that uses policy instruments. This approach permits to clearly identify the differences.

An assessment of GDPR-compliance in absence of a policy instrument is shown in Figure 4.

[12] In particular, according to Art. 40(5) GDPR, these affected controllers are members of the association or other body who submits a draft CoC for assessment and approval to a supervisory authority.
[13] The many affected controllers can include data access bodies (e.g. of different Member States) and data users who for certain processing tasks may act as joint controllers (see for example Art. 51 EHDS proposal).
[14] According to Art. 37(1)(g) EHDS proposal, the secure operating is provided by a health data access body.
[15] Note that for the case of CoCs, the EDPB lists "confidence and legal certainty" as one of the benefits of Codes of Conduct (see Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, paragraph 15 on page 9).

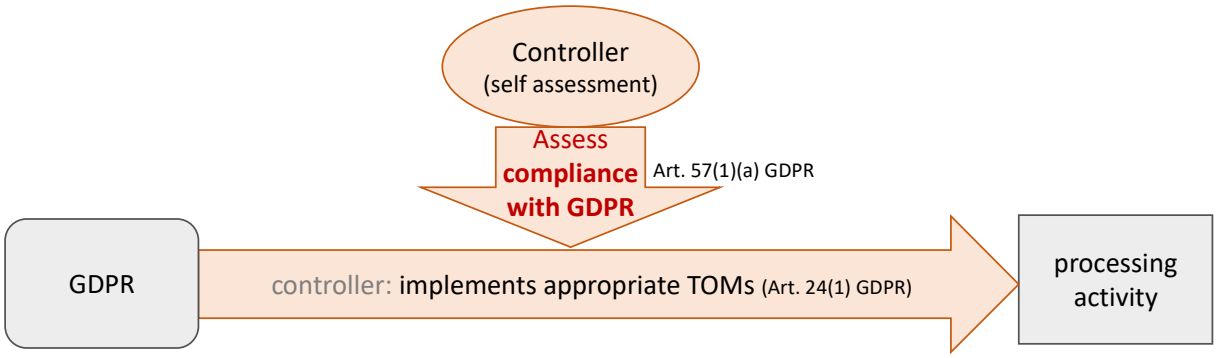

Figure 4: Assessment of GDPR-compliance in absence of a policy instrument.

According to Article 24(1) GDPR, as part of setting up a processing activity[16], "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation". In the following, the term *Technical and organizational measures* is abbreviated as *TOM*s.

GDPR-compliance can be assessed by different actors including the competent Supervisory Authority or a court. The Figure shows the controller itself as (self-)assessor. According to Art. 25(1) GDPR, TOMs "are designed to **implement data-protection principles** […] *in an effective manner* **and** to integrate the ***necessary* safeguards** into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". Key to understanding the assessment aspect of this statement lies in the wording of "in an effective manner" and "necessary". (These parts are shown in italic in the citation). In other words, the compliance assesses whether the implemented TOMs adequately mitigate the risks to the rights and freedoms of natural persons that are created by the processing activity. In essence, the assessment of GDPR-compliance is an evaluation of the effectiveness of the mitigation provided by the implemented measures.

Such an evaluation usually requires a significant degree of expertise, both, in technical and legal questions. It also typically involves the balancing of relevant interests and rights. This kind of balancing is commonly used in legal analysis. The assessment of GDPR compliance is therefore often a multi-disciplinary task that requires ample interpretation of the legal text as it applies to a concrete situation.

In comparison to Figure 4, the assessment of GDPR-compliance that uses a CoC is shown in Figure 5. While a CoC is a specific policy instrument, it can be seen as a prototypical situation that applies to all discussed policy instruments. The benefit of using a CoC instead of a generic policy instrument renders it possible to provide references into the GDPR and thus further sustain the process depicted in the figure.

[16] Legally, "setting up" is equivalent to "determining the purposes and means".

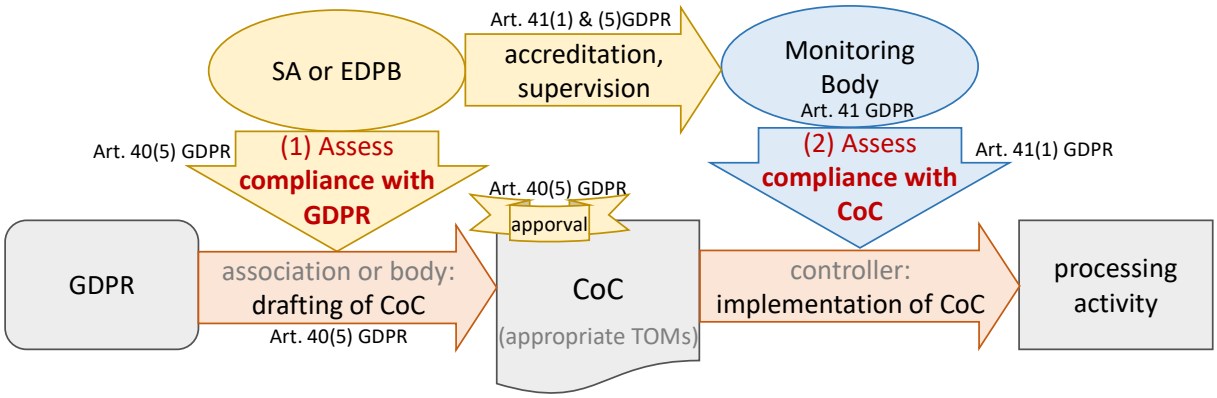

Figure 5: Assessment of GDPR-compliance that uses a Code of Conduct.

As shown in the figure, the overall assessment of GDPR-compliance is now performed in two steps:

- In a **first step** the (partial) **GDPR-compliance of a policy instrument** (such as a CoC) is assessed;
- in a **second step**, the **compliance of a concrete processing activity with the policy instrument itself** is checked.

The first step of assessing the policy instrument is similarly complex and requires a comparable level of expertise as the assessment without the use of policy instruments shown in Figure 4. In contrast, the second step of assessing the compliance with the policy instrument itself can be designed to be far easier in order to require less expertise.

The main benefit of using policy instruments originate from this difference in complexity. In particular, providing an economy of scale, the cost and effort that goes in the complex first assessment step can be reused many times for multiple processing activities in many far less complex second assessment steps. The expertise required for the second assessment is significantly lower. This means for example that *monitoring bodies* of CoCs do not require the full expertise of a Supervisory Authority. It permits larger controllers to partly delegate implementation to technical staff without legal skills. It also renders SMEs with only limited data protection expertise to reach compliance easier and at a lower cost. In other words, the first assessment step "stores" the result of a complex analysis to be used multiple times in step 2 assessments.

5.4 Factors that render policy instruments effective

This section discusses some factors that render policy instrument effective. Their maximization leads to a maximization of how a policy instrument can facilitate operationalization.

5.4.1 Focus on easy assessment of the policy instrument itself

The first characteristic is a **clear focus on** the main objective that is to guide the **assessment of compliance with the policy instrument itself** (i.e., the second assessment step in Figure 5). The objective is to make such assessment as easy as possible. As is evident from Table 1, all instruments have the objective of supporting the assessment of the compliance with its own prescriptions. In the

case of CoCs, for example, this is explicitly stated in Art. 41(1). It is also the case for self-assessment by controllers of the compliance with an internal policy[17].

To render it easy to assess compliance with a policy instrument, it must address the following aspects:

1. **Specified requirements** (aka. a criteria catalog);
2. **requirements for eligible assessors** (e.g., minimal qualifications or experience);
3. **the basis** on which requirements are evaluated (e.g., based on *documentation*, an *onsite audit*, *interviews*, *system configuration*, *activity logs*, or *accessing a system as a user*, etc.).
4. clear **rules, procedures,** and **methodology** of how to assess the individual requirements; and
5. **rules on the composition** of such individual assessments into a single overall assessment outcome of the policy instrument. The overall assessment could for example be based on the rule that each individual requirement must be satisfied or that it is sufficient that only a specified percentage of requirements is satisfied[18].

In all cases, the **outcome** of an assessment a policy instrument is **always either *pass* or *fail***. For example, a certificate is either issued or denied. In the latter case, a precise justification in form of listing the failed individual requirements constitutes a helpful addition to the main assessment result.

5.4.2 Minimization of room for interpretation

A second factor of effectiveness is **the minimization of the room for interpretation** available to assessors **and** the minimization of the **degree of subjective judgement**. The objective is to guarantee that different assessors come to the same outcome when assessing the same processing activity. Similarly, the outcomes for comparable processing activities should be the same. In other words, the assessment of the instrument should be **reproducible** and **consistent**. It is evident, that any room for interpretation or subjective judgement endangers this objective. This factor of effectiveness can also be seen as requiring a very high level of concreteness. Ideally, the assessment of criteria should be almost "mechanical"[19] and provide so much concrete and precise instruction that outcomes are very likely consistent.

5.4.3 Minimization of interdisciplinary assessment

A third factor of effectiveness is the **minimization of any need for interdisciplinary evaluation**. This is of particular importance considering that data protection is inherently an interdisciplinary field that requires both, legal and technical expertise. Interdisciplinary assessment is a major source of inconsistency. In particular, it typically requires two or more persons to execute the assessment. To reach a reproducible and consistent assessment, the participants likely need a shared common understanding, communicate in a mutually understood terminology[20], and eliminate the individual

[17] Such self-assessment that is implies in Art. 24(2) GDPR partially fulfills the requirements of Art. 5(2) GDPR "accountability".

[18] While these examples are very simple, the composition of results for individual requirement to an overall assessment result can be arbitrarily complex.

[19] Note that this does not mean that there cannot be professional judgement or balancing as part of the evaluation.

[20] Note that the legal and the technical understanding of the same term can be different. Some differences are evident and can probably be easily managed, others may be too subtle to detect but significant for the outcome of an assessment. An example for a term that is understood differently is "pseudonymization". In the technical field, this is a transformation of data while legally, according to Art. 4(5) GDPR, it is a manner of

strength of character from the determination of decisions[21]. This is difficult to achieve and adds considerable complexity.

While the overall assessment of GDPR compliance is clearly interdisciplinary, the author of effective policy instruments should break the assessment down into a multitude of assessments of individual requirements, each of which requires only the expertise of a single discipline. For example, to assess whether a certain form of encryption is adequate in the context of a concrete processing activity, a legal professional may determine the necessary level of protection and a technical professional then assesses whether the actual technical implementation reaches this level.

5.5 Proposed structure and content of policy instruments

The following proposes a structure and necessary content for policy instruments. The proposal is based on the above discussion of the assessment process and factor of effectiveness of policy instruments.

Figure 6 shows the proposal. This section further describes its structure and elements in further detail.

The figure employs a reddish background color to highlight the fields that are at the core of the actual assessment of processing activities. Fields targeted at assessors of the policy instrument (most notably supervisory authorities) much rather than the assessors of a processing activity are marked by a yellow background.

processing and the technical meaning is called "pseudonymising transformation" in the EDPB's Guidelines on Pseudonymization.

[21] For example, the situation where a very experienced legal professional works with a junior technical expert may lead to a different outcome than if the experience levels are swapped. In assessments that require a multidisciplinary team, it is difficult to eliminate any influence of seniority on the outcome.

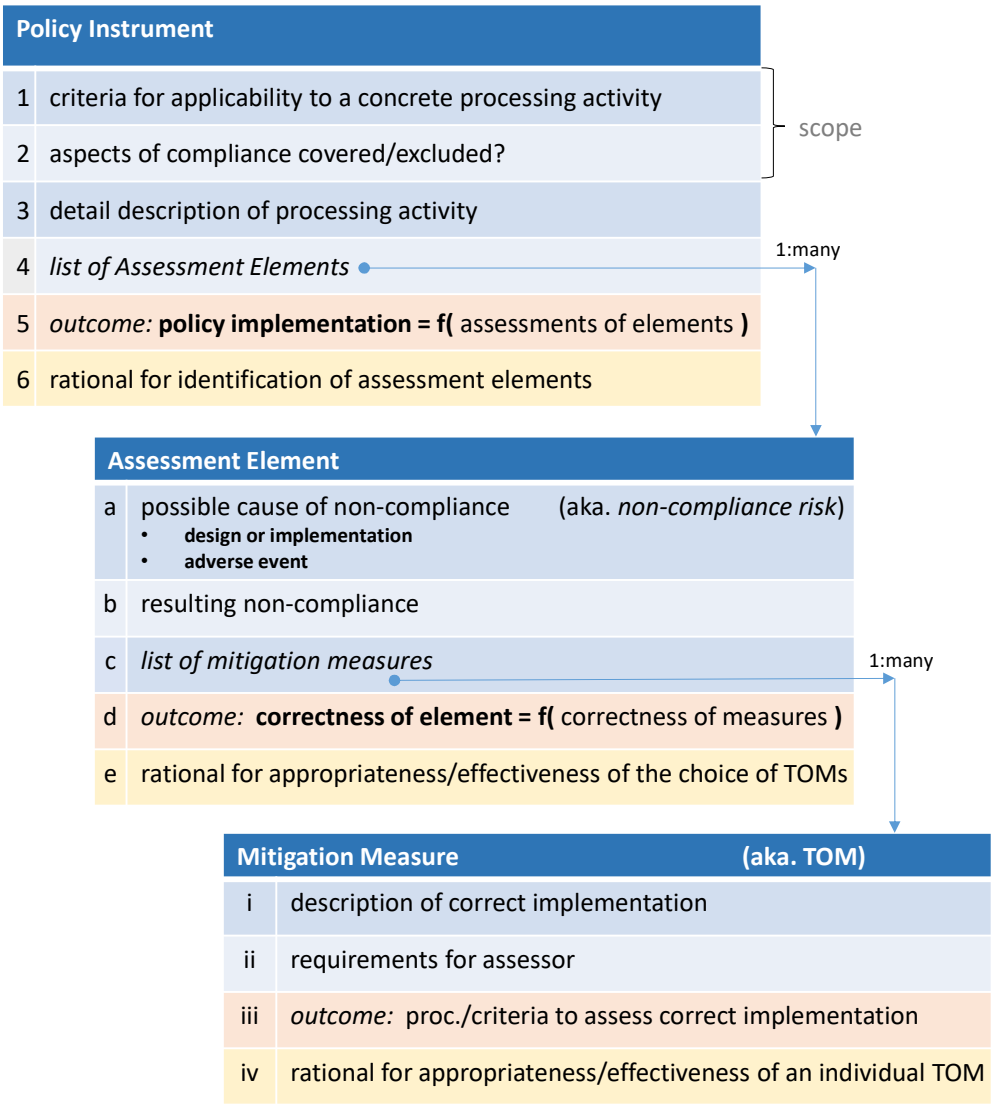

Figure 6: Proposed structure and content of policy instruments.

The content of a policy instrument is organized in a hierarchical structure. In particular, a policy instrument contains multiple *assessment elements*, each of which requires a multitude of *mitigation measures*. The remainder of this section describes the key content of these three main components. Only the content elements that are relevant to the present discussion are shown. Additional content elements, such as meta data[22] of the policy can easily be added.

(1) The first shown content field of policy instruments should support the decision of whether the instrument is applicable to a processing activity at hand. While it may also be possible to make this decision based on the detailed description of the processing activity (see 3rd content field), the present field should render it possible to make at least a tentative decision based on less detail by applying a number of criteria.

(2) Policy instruments often consider only a subset of requirements from the GDPR. This content field clearly states what aspects or parts of GDPR compliance the policy instrument can deliver.

[22] Meta data could for example comprise the owner, authors, version, contact information, a summary of required staffing, information about possible approval, etc. Similarly, a section of reference could be added. A name or id to uniquely reference a policy instrument are also left out to keep the figure simple.

(3) A detailed description of the processing activity that is assessed provides the necessary context to the instrument user (see step 2 in Figure 5) that helps understand where and how the later describe TOMs must be implemented. The description should among other address the following:

- The overall architecture of the processing activity with all its components
- Data flows, protocols (e.g. as sequence diagrams), and APIs that describe the interactions of components.
- Data flows to any 3rd party.
- The personal data processed in components and used in data flows.

In addition, in support of parties that evaluate and possibly certify the ability of the policy instrument to achieve GDPR-compliance see step 1 in Figure 5), additional elements include (see also Art. 24(1) and 25(1) GDPR)[23]:

- The assumed state of the art;
- relevant information regarding the cost of implementation;
- the nature,
- scope,
- context, and
- purposes of processing.

(4) A main content field for the assessment is a list of *assessment elements*.

(5) The policy must explicitly state how the outcomes of the individual assessments of these elements compose into an overall outcome for the whole policy instrument. This is visualized in the figure by using a the notation of a function, i.e., *f().* This function takes all the outcomes of the assessments of individual *assessment elements* as input.

(6) Together with the fields (e) and (iv), this field justifies how the identification of assessment elements in regard to overall compliance with the GDPR. It is thus targeted at parties such as supervisory authorities who assess the policy instrument (much rather than a processing activity). This field provides the rationale that all risks and compliance requirements that are in the scope of the policy instrument (see fields (1) and (2)) have been correctly identified.

The following describes the content of assessment elements:

(a) The defining property of an *assessment element* is a possible cause of non-compliance. This cause can lie in the design and implementation of the processing activity (i.e., legally the "determination of purposes and means") or in an adverse event. Examples for the former case is the failure to sufficiently implement the principle of 'data minimization' (see Art. 5(1)(c) GDPR) in the design and failure to implement data subject rights. Examples for the latter case are events such as attacks, HW failures, SW bugs, and data errors that can occur

[23] A description of the possible content for these properties was propose by the PANELFIT Project in the context of a DPIA (see https://guidelines.panelfit.eu/the-gdpr/main-tools-and-actions/dpia/is-there-a-standardized-method-for-carrying-out-a-dpia-are-there-outlines-templates-or-tools-in-support-of-carrying-out-a-dpia/)

with a certain probability and cause non-compliance with requirements such as the principle of 'integrity and confidentiality' (see Articles 5(1)(f) and 32 GDPR).
This field could also be considered to be the description of a 'non-compliance risk' or a risk to the rights and freedoms of natural persons.

(b) While the previous field described a cause, the present field describes the consequences of the cause realizing itself. This can be a violation of a GDPR principle (see Art. 5 GDPR) or of a more detailed requirement such as a data subject right (see Articles 15 through 22 GDPR). It could further encompass additional possibly caused physical, material or non-material damage to data subjects (see Recital 75 GDPR).

(c) This field provides a list of technical and organizational measures that are deemed appropriate by the author of the policy tool to adequately mitigate the risks described in (a). This is subject to a correct implementation of the measure as is assessed in (iii).

(d) Similarly to (5), this field explicitly state how the overall outcome of the *assessment element* is composed from the individual assessments of *mitigation measures* in (iii).

(e) Together with (iv), this field justifies how the choice of TOMs contributes to overall compliance with the GDPR. It is thus targeted at parties such as supervisory authorities who assess the policy instrument (much rather than a processing activity). This field provides the rational why the chosen TOMs are appropriate and sufficient to mitigate the risks referred to by Art. 24 GDPR.

The following describes the content of mitigation measures:

(i) The description of correct implementation of a *mitigation measure* aims to provide controllers with precise instructions of how to comply with the policy instrument by correctly implementing each mitigation measure.

(ii) This field describes the requirements, such as qualifications or level of experience, for a person to be able to assess the correct implementation of a technical or organizational measure. This field must thus clarify the discipline that is necessary for the assessment. In particular, in data protection, it must be clear whether the assessment is a legal or a technical task.

(iii) This field is at the core of assessing compliance with the policy instrument itself. In particular the field provides precise instructions of how an assessor has to evaluate the correct implementation of the prescribed measure. These instructions must contain both, **criteria of evolution** as well as specifying the **basis of assessment** (such as documentation or an on-site inspection of some system) and **precise procedure and methodology** used in the application of the criteria (see also section 5.4.1 above). The objective of this field is to render the assessment as **objective** and **reproducible** as possible such that outcomes become consistent across all possible assessors. A second objective is to require as little competence as possible of the assessor. The assessment should aim to be "easy" since complex assessment typically leads to inconsistencies.

(iv) This field complements the reasoning provided in field (e) from the point of view of a single measure. The audience of this field are thus not assessors of compliance with the policy instrument but rather the assessors of the policy instrument in regard to GDPR-compliance. For example, this field may address a supervisory authority to whom a CoC

was submitted for approval. While field (iii) is designed to provide easy instructions for persons with limited data protection expertise, this field is written for an audience with a very high level of data protection expertise. It can well also contain interdisciplinary reasoning. The text provided by the policy author should facilitate the assessment of the policy. Therefore, the field typically describes how the measure in object contributes to the obligation of controllers to appropriately mitigate the risks to the rights and freedoms of natural persons (see Art. 24(1) GDPR).

The presented proposal for a structure and content of policy instruments has no ambition to be final, but it aims at contributing to the discussion of what it takes to render policy instruments effective tools of the operationalization of data protection.

5.6 Conclusions about Policy Instruments

This essay has analyzed the role of policy instruments for the purpose of operationalization data protection legislation. In particular, it has generalized multiple policy instruments (such as controller-internal policies, Codes of Conduct, and compliance assessment schemes) into a single generic concept of *police instrument*. Pointing out the similarities in their purpose and role has allowed to propose a single structure and content for all these instruments. The essay has discussed factors that are crucial for effective operationalization and attempted to embed these into the proposed structure and content.

The unique selling point of unapproved policy instruments is the economy of scale that they can bring to a controller; that of a formally approved policy instrument is the increased confidence and legal certainty[24] that it brings. For these reasons, the authors expect that the emergence of such instruments will have a significant impact on the operationalization of data protection legislation.

This essay was written with the objective to encourage the drawing up of policy instruments as stated in Articles 40(1) and 42(2) GDPR. The authors hope to contribute to a wider discussion on how to best achieve this objective and how different actors can best contribute.

6 Conclusions

This deliverable has reported on the results of the work in the Task 4.9.3 of the AnoMed project. The main result is a concept of how to enable secondary use of personal data in a GDPR compliant manner. This is reported in Section 4. In addition, the work has yielded results on a meta-level. In particular, the question about how the actual result (the "concept") can be presented in a way that potentially create impact beyond just the project has been addressed in two ways:

(i) experimentation of a suitable format that resulted in the structure of the concept description in Section 4;
(ii) a generalization of this experience that is potentially applicable to render future research work more impactful and can potentially guide data protection practitioners in how to write effective policies, codes of conduct, and similar policy instruments.

[24] Note that the increased confidence and legal certainty can make a significant difference to an entrepreneur's decision whether to invest into an endeavor that involved personal data.