D5.4 Final Advanced Cloud Service meta-Intermediator (Annex)

White paper on the non-functional requirement of a legal level assigned to every Cloud service in DECIDE's Advanced Cloud Service meta-Intermediator (ACSmI)

Editor(s):	Pieter Gryffroy
Responsible Partner:	Timelex
Status-Version:	V1.0 – Final
Date:	31/05/2019
Distribution level (CO, PU):	PU

Project Number:	GA 731533
Project Title:	DECIDE

Workpackage responsible for the Deliverable:	WP5
Editor(s):	Timelex
Contributor(s):	Pieter Gryffroy (timelex)
Reviewer(s):	Manuel León; ARSYS
Approved by:	All Partners
Recommended/mandatory readers:	WP 5, other technical WPs as needed.

Abstract:	This deliverable contains the final version of the implementation of the Advanced Cloud Service meta-Intermediator (ACSmI)). This deliverable is the result of T5.1 – T5.5. The software will be accompanied by a Technical Specification Report. This document is an annex that contains a White paper on the concept of the legal level in ACSmI and its implementation, including an explanation of the controls making up the legal level, the procedure involved in assigning the legal level, a proof of concept and some use cases.
Keyword List:	Whitepaper, legal level, ACSmI, compliance, legal aspects
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) http://creativecommons.org/licenses/by-sa/3.0/
Disclaimer	This document reflects only the author's views and the Commission is not responsible for any use that may be made of the information contained therein

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	02/04/2019	First draft version finished	Timelex
v0.2	05/04/2019	Comments and suggestions received by consortium partners in GA	ALL
V0.3	15/05/2019	Final version of the white paper	Timelex
V0.4	16/05/2019	Small changes after review	TECNALIA
V0.5	23/05/2019	Review	ARSYS
V0.6	27/05/2019	Version after internal review	TECNALIA

Table of Contents

List of Tables

Terms and abbreviations

A	Article
ACSmI	Advanced Cloud Service meta-Intermediator (DECIDE tool)
ADR	Alternative Dispute Resolution (mechanisms)
CCSM	Cloud Certification Schemes Metaframework
CEO	Chief Executive Officer
CoC	Code of Conduct
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
D	Deliverable
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EBA	European Banking Authority
EEA	European Economic Area
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
M	Month
NFR	Non-functional requirement
OCF	Open Certification Framework
SLA	Service Level Agreement
SME	Small and medium-sized enterprise

Executive Summary

This white paper is an annex of the D5.4 (Final Advanced Cloud Service meta-Intermediator (ACSmI)), delivered M30. It should be read in conjunction with that document and other DECIDE deliverables.

It aims to explain the approach to one of the aspects of ACSmI, namely the assigning and monitoring of a legal level for each Cloud service when onboarding them in ACSmI, which may then be used as a non-functional requirement by the application developer, thereby ensuring that the multi-cloud application is only deployed with the use of Cloud services which meet the required legal level.

The whitepaper explains the concept and approach of the legal level. It also provides a proof of concept and some use cases. In addition, it describes the contractual framework that will make the legal level operational and provides basic input for the technical implementation.

The white paper finishes with some remarks on sustainability and upscaling for the future.

1. Introduction

This document is the legal level white paper written to accompany deliverable D5.4, which contains a section on the legal level assigned to Cloud services in ACSmI. It builds on the findings presented in deliverable D5.3.

The white paper aims to:

- explain the approach for the legal level
- provide some guidance on the application of the legal level
- provide context surrounding its development
- look at some essential side questions, such as the necessary contractual documents to be put in place between DECIDE and its users to make the legal level operational in practice, and the implementation of the legal level in the future

The document is written order to explain the approach taken to define a legal level functionality in DECIDE to help the application developer differentiate between Cloud services.

However, it is important to take into account that while the application developer may be the only real user of the DECIDE framework, the developer always is working for a target user organization (to which he/she may or may not belong), or even organizations, as the case may be when a commercial product is being developed meant for sale to several target user organizations, i.e. clients (bespoke product) or customers (general commercial product).

Consequently, when trying to describe the reasoning behind and the functioning of the legal level functionality in DECIDE, it is always with both the application developer as well as the final target user organizations in mind.

When referencing a “DECIDE user” however, this means the application developer alone. When referencing the application developer, reference is meant to be made to the organization developing, not a specific natural person, although the organization will at all times need to act through a specific person.

This reality also means that the application developer’s organization will be the controller under the GDPR when developing for in-house use, but will be a processor when developing for a client. This does not affect the contracts offered by the CSP, as they very well know that their clients are often not controller in the end. The contracts offered by the CSP are offered to their customers, and thus the contractual commitments are not affected by the application developer changing roles from controller to processor. This does however entail an important shift for the application developer, as they must take into account that their contractual relationship with the client is heavily affected by the contracts it has with DECIDE and/or with the CSPs (depending on whether ACSmI will act as a reseller or more like Cloud broker brokering direct contracts with the CSPs).

Nonetheless, in both scenarios the legal level will have a clear value in facilitating the choice of CSPs and Cloud services, by assigning a legal level to each Cloud service and defining guarantees for each legal level, thus enabling the application developer to define legal needs for the target user organizations, to pick the matching legal level tier based on those needs (i.e. the tier that provides sufficient guarantees) and thus to easily pre-select only Cloud services that meet these requirements in ACSmI to deploy the multi-Cloud application, given that the legal level functions as an NFR in ACSmI, filtering potential options in the catalogue.

The following sections explain the functioning of the legal level, provide a proof of concept, use cases and context surrounding the implementation of the legal level.

1.1 About this white paper

This white paper is an addition to deliverable D5.4, meant to clarify the approach taken to the legal level functionality in ACSmI.

1.2 Document structure

The document has the following structure.

First, section 2 explains the legal level in ACSmI in detail, touching upon:

- The overarching concept (section 2.1); and
- The controls of which the legal level is composed (section 2.2 and subsections); and
- Some general consideration on the legal level and the choices made in definition of the concept and selection of controls (section 2.3 and subsections); and
- The legal matrix, which shows the guarantees offered by each tier for each control (section 2.4 and 2.5); and
- Information on how the legal level is assigned and monitored in ACSmI (section 2.6); and
- Information on the NFR function of the legal level in ACSmI (section 2.7); and
- A proof of concept (section 2.8); and
- Use cases for the legal level (section 2.9).

Second, section 3 provides a legal framework for the legal level to be implemented.

Section 4 follows with some input for the technical implementation of the legal level in ACSmI, called the ACSmI legal awareness component.

Section 5 wraps up the white paper by providing some notes on sustainability and scalability of the legal level for the future, followed by the formal conclusion in section 6.

2. A legal level for Cloud services in ACSmI

2.1 Conceptual approach

The legal level as a concept was already partially explained in D5.3. It is a concept that allows categorizing Cloud services in ACSmI and differentiating between them based on the level of legal safeguards they offer. The legal level contains three tiers, ranging from tier 3 as a basic standard to tier 1 which provides for a high level of legal safeguards. Cloud services that fail to meet the requirements of the basic tier 3 are not allowed to be onboarded in ACSmI.

In its section 7 on the legal level in ACSmI, deliverable D5.3 explained the struggle in defining a legal level for Cloud Services which is applicable in an abstract sense, i.e. relevant to any and every user of DECIDE's framework, without knowing the specific background of the application developer's target audience, i.e. the intended user organizations of the multi-Cloud application. It explained that the value of some legally relevant aspects (e.g. the value of a certain certification) are in the eyes of the beholder, and therefore hard to assess *in abstracto*.

From this finding D5.3 reasoned that only certain legal topics should be taken into account in the determination in the legal level, namely those on which information could be obtained which could be assessed *in concreto*, in the first place based on the contractual documents CSPs are required to upload when onboarding their service into ACSmI, and on the other hand other pieces of information that CSPs might be required to provide in addition to those contracts, i.e. by answering a limited list of questions to obtain legal information which is relevant but not (typically) expressly provided in a contract (e.g. the presence of a DPO at the CSP). Through answering a much more extensive list of questions based on the information obtained from both the uploaded contracts and the limited question list answered by the CSP, the legal expert would then be able to determine the legal level.

A remaining issue at that time was how to define the weight and importance of each of the topics covered, since even generally relevant legal aspects which can be assessed on the basis of information provided by the CSP might have a different importance based on the specific needs of the target user organizations. One method that was suggested was to calculate legal levels based on a mathematical point system. The issue with that, however, is that it still presupposes that a general weight or importance can be given to certain legal topics. An advanced understanding of this issue reveals that such a mathematical system would only be superior when objective factors are known on the basis of which weight/importance can be assigned or, conversely, subjective factors relevant to a specific target user organization or group of organizations, for which the point system could be designed specifically. While this may be something that can relevant for the future (see on this section 5), it is not a workable solution for the general legal level in ACSmI.

A better option therefore, is to define a set of legally relevant controls based on the identified legal topics and to differentiate between legal levels tier 1 (highest level – strong legal safeguards), 2 (medium level – substantial legal safeguards) and 3 (lowest level – basic legal safeguards) based on the extent to which they fulfill these legally relevant controls.

Two types of controls can be imagined.

A first type of legally relevant control will rely on a yes/no question, essentially asking whether something is in place or not (e.g. is there a DPO?). They are referred to further as "simple controls".

Simple controls can contribute to the legal level of the Cloud service by simply being substantively present. The more controls of this type a service can "check", the higher the legal level will be. The basic principle can be graphically represented as follows in a matrix, marking the controls that are present with a green check mark and those that are not with a red cross mark:

Table 1. Simple controls example matrix

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
Control 1	✓	✓	✓
Control 2	✓	✓	✓
Control 3	✓	✓	✓
Control 4	✗	✓	✓
Control 5	✗	✗	✓

In a way the determination of which are the basic controls that need to be present and which additional controls justify and upgrade to tier 2 and tier 3 will be arbitrary. This does not mean that there will not be any reasoning provided, but rather that our determination of what is a tier 3, tier 2 and tier 1 service may differ from what the user organizations of multi-Cloud applications provided through DECIDE may consider to be relevant for themselves. Taking the example above, a user organization could consider controls 1 and 4 to be elementary, constituting the base level (i.e. tier 3). This would then force them to select legal level tier 2 in order to have both controls, thereby adding controls 2 and 3 which they did not really care about. This is exactly the problem described above of trying to provide an abstract legal assessment for all potential DECIDE users, although their specific legal requirements will greatly differ. This approach however, has the benefit of enabling the user organization and/or the application developer to determine in full transparency which legal level fulfills all of its perceived needs by providing the controls they consider relevant. None of these controls is given a weight/importance by DECIDE or the legal expert. Their value and importance is decided by the application developer and/or the target user organization(s). The legal level only specifies which controls are present, enabling the right choice. Since the legal level in no way impacts any other characteristics of the service (e.g. cost or availability), the worst case scenario of a mismatch between our interpretation of the tiers of the legal level and that of an user organization would be that the user organization is forced to take a Cloud service of a legal level tier which provides more controls than actually perceived as necessary, thus potentially limiting their subsequent choice of Cloud services in ACSmI, although this might be more theoretical than a real concern.

However, not all controls can be assessed in this straightforward manner of ascertaining (or rather, asking the CSP to confirm) whether they are substantially present or not. Some controls will need to be more differentiated, assigning a value to the specific manner in which the control is fulfilled. An example is the auditing rights required by Article 28(3) of the General Data Protection Regulation [1] (further: GDPR) as part of a data processing agreement. Many specific clauses exist amongst CSP contracts and not all these clauses assign the same rights, nor are they all necessarily compliant with the GDPR. Therefore, assessing that a clause is present in the contractual relationship with the CSP is not sufficient. Some auditing clauses will be very restrictive and may only allow the user organization/controller to request a copy of the auditing report of the CSP's usual auditor. Others may allow the user organization/controller to conduct their own physical audits at the CSP's premises. This may be relevant for the user organization for many reasons, amongst which general GDPR compliance, but could equally be a regulatory requirement for the user organization/controller in certain sectors, based on (national) specific legal requirements in those sectors.

These controls are further referred to as "layered controls".

Layered controls need to be assigned a value. In order to do these three levels of compliance can be defined for such controls (typically consisting of contractual guarantees):

- Controls that are faulty, provide a low level of protection, or are otherwise clearly less than ideal, but seem to be sufficiently conforming to the applicable law to not be an immediate compliance issue are labelled “low protection”.

- Controls that are adequately described, enforceable and provide a more or less balanced level of protection and obligations and rights are labelled “medium protection”.

- Controls that are adequately described, enforceable and provide a strong protection and rights for the application developer/target user organization, are labelled “high protection”.

Controls that do not at least meet the level of “low protection” are considered to be not present at all. In a matrix of controls, stars could be used to graphically represent the level of protection. Low protection would then be represented by a single star, medium protection by two stars and high protection by three stars, as follows:

Table 2. Layered controls example matrix

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
Control 6	★	★★	★★★
Control 7	★	★★	★★★
Control 8	★	★★	★★★
Control 9	★	★★	★★★
Control 10	★	★★	★★★

Put together, the legal level matrix will be based on a combination of both types of controls, giving a result that would look as follows:

Table 3. Combined controls legal level example matrix

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
Control 1	✓	✓	✓
Control 2	✓	✓	✓
Control 3	✓	✓	✓
Control 4	✗	✓	✓
Control 5	✗	✗	✓
Control 6	★	★★	★★★
Control 7	★	★★	★★★
Control 8	★	★★	★★★
Control 9	★	★★	★★★
Control 10	★	★★	★★★

This is of course a simplified representation to illustrate the principle.

As explained in D5.3 [2], the legal level is assigned by the DECIDE legal expert. This is based on a review of the contracts uploaded by the CSP combined with an analysis of the additional questions answered by the CSP.

In D5.3, it was stated that the legal expert will be guided in the contract assessment by questions per relevant topic. These questions will be defined below per topic, i.e. per control.

The legal expert will take into account all information in ACSmI's legislation awareness component in order to conduct the contract reviews.

In addition to that, the CSP will have to answer some questions to provide additional information not present in the contracts. These questions will exclusively be related to simple controls and are aimed at finding out whether the CSP has a measure in place or not.

The legal expert will thus make up a score for every service and assign the legal level that matches that score by awarding the service the highest level for which it reaches all the provided values. In other words, the legal level will guarantee that a given service has *at least* the qualifications that are said to be part of the tier of the legal level in question. See more on this in section 2.5 which provides the final matrix for the legal level and accompanying explanation.

Each service, when being onboarded/endorsed in ACSmI, will be assigned a legal level by the legal expert.

During the onboarding the CSP will have to:

- upload both its contractual documents
    - service contract
    - specific terms
    - data processing agreements
    - other contractual documents (SLA, acceptable use policy, etc.)
- answer the list of additional questions.

Both types of information (contracts and additional information through answering the questions) are intended to be legally binding on the CSP through a contract. This would also enable an obligation for the CSP to inform the legal expert/the entity exploiting ACSmI on any relevant changes. See section 3 on this. Although this information may largely be gathered from the Internet, it is preferable to have the CSP actively engaged in the process for obvious reasons. However, onboarding a CSP is technically possible in ACSmI without CSP engagement (see section 2.6.1 on this).

The combination of this information will enable the legal expert to assign the Service its legal level.

After analysis the legal expert will assign the correct legal level. See section 2.6 for more information

If the CSP does not agree with the legal level that is assigned, there is a procedure foreseen to address that. See section 2.6 for more information.

After a service has been endorsed in ACSmI and has thus received its legal level, there will be only limited events that trigger the re-assessment of the service. See section 2.6 for more information on this.

The contracts underlying the Cloud service will typically between the CSP and the application developer directly or between the application developer and the entity exploiting ACSmI, which then will have contract with the CSP. Thus, the application developer will not necessarily have a direct contract with the CSP. The same is true for the any clients or customers of the application developer, if the application developer is not developing for in-house use at the organization but making a general commercial or bespoke product (e.g. a SaaS solution).

In these cases, the controller in the sense of the GDPR may not be directly involved in the contract with the CSP. The fact that their customers are often not the controller at all is a reality that CSPs are aware of but does not address because it is much easier to just qualify all contractual relationships as a controller-processor relationship where they are the processor. Thus, the guarantees they offer the

"controller" is really just guarantees they offer their customers. Moreover, it may often be impossible at the time of the contracting of the Cloud service to determine which organization(s) will be the controller of the final processing, and thus be impossible to have contracts with them. That is why the legal level generally refers to "the CSP's counterparty", so as to indicate the reality that the CSP's counterparty, which is either the application developer or ACSmI, is not necessarily the controller (and in the case of ACSmI necessarily not).

In the case where the application developer is the controller, it has to have data processing agreements with both the CSPs it directly contracts with and with ACSmI for the Cloud services it should contract through ACSmI, which will pass on the guarantees it itself gets from the CSPs.

The legal level can be useful in this situation to assess what guarantees one will obtain as a minimum from either ACSmI or the CSP directly.

Where the application developer ends up being a processor for its clients/customers, it is important to realize that the developer will become the first processor for the clients/customer who will be the controller. Thus, there will need to be a data processing agreement between them that will need to be reflected down the chain (per Article 28(4) GDPR). Since many CSPs use standard contracts, the application developer will essentially need to start from those contracts and promise only what the CSPs guarantee him, failing which the application developer would assume all the risk and enter into a situation of non-compliance.

In this situation the legal level is obviously helpful in selecting CSPs that offer a certain level of legal compliance that then can be passed on to its customers/clients.

See section 2.9 on use cases of the legal level and how the legal level can be used by different organizations based on their identified needs.

See section 3 on the legal framework between the application developer as a DECIDE user, the DECIDE alliance/the entity exploiting ACSmI and the CSPs.

2.2 Controls used for the determination of the legal level

In the following sub-sections, the controls that are part of the legal level matrix are explained. As stated earlier, the controls are not given a specific weight or importance. It remains up to the application developer, and through the developer, the target user organizations to determine which controls they consider to be important, and based on this determination, which legal level they prefer for the multi-Cloud application.

The structure of each of the following sub-sections is the same.

- First, the control is described in more detail. Some controls are marked as "if relevant". This signifies that the control is only relevant in a given situation or if a certain clause is present in the contractual documents, in the absence of which the control is not useful;
- Second, the control is defined as either a simple control or a layered control. The determination of this will determine the questions that are defined in the third step;
- Third, a question is defined to assess the control:
    - For simple controls, this will be yes/no questions aimed at the CSP. As explained before and in section 2.6 and section 3, there's the intention of the consortium to actively engage CSPs to the extent possible, although it is technical possible for ACSmI admins to go through this process independent of the CSP.

      The CSP will answer these questions during the onboarding process and the legal expert will account for the given answer in determining the legal level.

      Positive answers will lead to the control being marked as present (a green check mark in the legal level matrix), while negative answers will lead to controls being marked as not present (a red cross mark in the legal level matrix).

      If the control is not applicable to the service at all, as is possible with the controls relating to data exports outside the EEA, then the control will not need to be answered and will not be counted towards the legal level. See section 2.5 for more information.
    - For layered controls, the question will be aimed at the legal expert, which should answer the question based on the contractual documents provided by the CSP. The question guides the legal expert in the legal review of the contractual documents, needed to assign the legal level offered by the Cloud service. It is important that this assessment is conducted following pre-defined guidelines so as to make it transparent for the CSP.

      The legal expert will use the guidance provided in the controls and other guidance and consistency instructions provided for this. The legal expert will also provide justification for every answer chose, which may be reviewed by the CSP.

      See section 2.6 for details on this and section 3 for the contractual framework enabling this.

      Layered controls can have four potential results.

        - The lowest result is a situation of non-compliance, i.e. serious issues. This will lead to zero stars being awarded, which will be represented in the matrix with a red cross mark, indicating that the minimum level of protection (i.e. low protection, represented by one star) is not present.

- The second lowest result is a situation of low protection for the application developer/target user organization. It will be marked with one star in the legal level matrix.
- The next result is a situation of medium protection for the application developer/target user organization. It will be marked with two stars in the legal level matrix.
- The best result is a situation of high protection for the application developer/target user organization. It will be marked with three stars in the legal level matrix.

Some controls are only relevant in certain situations. They are marked “if relevant”. If not relevant, those controls need not be addressed by the legal expert and they are not counted towards the result of the legal level. See section 2.5 for more information.

- Fourth the potential answers are listed.
  - For the simple controls, first the positive answer is listed, then the negative, and, when applicable the third option that the control does not apply to the service in question
  - For the layered controls, the answers will be given from lowest (non-compliance) to highest (high protection).

  In the implementation of the legal level in the tool, this order may be changed.
- Fifth, a short explanation is given justifying the inclusion of the control in the legal level assessment.

2.2.1 Valid company registration

Control	**This control aims to ensure that the CSP is at least a valid registered and incorporated entity, excluding market players that do not operate under any entity, entities in liquidation or in a declared state of bankruptcy.**
Type	Simple
Question	Is your organization a validly registered and incorporated entity, which is neither in liquidation nor in a state of bankruptcy?
Possible answers	Yes
	No
Reason for inclusion	While this might seem like a given, it is essential for the CSP's counterparty to deal with a valid legal person, against which it might act if necessary. Without this basic guarantee, it would be unwise to engage in business with any actor.

2.2.2 Presence of a DPO/data protection point of contact

Control	**Presence of an appointed DPO in the sense of Articles 37-39 GPDR in the CSP's organization or an equivalent position, e.g. a privacy officer, or privacy team which can act as a data protection point of contact.**
Type	Simple
Question	Did your organization appoint and will it maintain a DPO in accordance with Articles 37-39 of the GDPR or an equivalent position e.g. a privacy officer or privacy team which can act as a data protection point of contact?
Possible answers	Yes
	No
Reason for inclusion	The appointment of a DPO at the CSP is a basic indication of how seriously the CSP is committed to data protection. Given that the controller (typically the target user organization) is tasked with engaging only reliable processors (Article 28 GDPR), this is a relevant fact to include in the legal level assessment. To accommodate the fact that CSPs are not necessarily formally obliged under the GDPR to appoint a DPO, it would suffice for the CSP to appoint an equivalent role or team that may fulfil the functions of the DPO, without qualifying the role as a DPO as such.

2.2.3 Presence of a representative in the EU (if relevant)

Control	**Presence of a representative in the EU of a CSP only established outside the EU, if relevant.**
Type	Simple
Question	Did your organization appoint and will it maintain a representative in accordance with Article 27 of the GDPR?
Possible answers	Yes.
	No.
	Not applicable.

Reason for inclusion	In those situations where a CSP does not have an establishment in the EU, the representative is a point of contact but also a replacement of the CSP for legal claims. This may be especially relevant in worst case scenarios where damages have to be recovered against the CSP, e.g. under Article 82 GDPR. In such a case, if no representative is appointed, it may be factually difficult to obtain any redress in the third country jurisdiction. The presence of a representative solves those issues and also, if and when required by the GDPR, shows a general basic level of commitment of the CSP to compliance.

2.2.4 Presence of a data transfer mechanism declared by the CSP (if relevant)

Control	**Presence of an adequate data transfer mechanism under the GDPR declared by the CSP in case of data transfers outside the EEA (i.e. the Cloud service hosts data outside the EEA), as prescribed in Articles 44-49 GDPR.** **Note: if the service is only performed in the EEA, this control is not considered.**
Type	Simple.
Question	In case data is transferred outside the EEA, do you have in place sufficient safeguards, as described in Articles 44-49 of the GDPR?
Possible answers	Yes.
	No.
	Not applicable.
Reason for inclusion	Data transfers have to be subject to adequate safeguards. This is a high compliance risk for the controller if not taken into account and therefore an essential point to include. It is included here as a simple control to have a binding statement on the side of the CSP, as well as to gather information on transfer mechanisms which may not necessarily be described in the contractual documents. This is necessary for the assessment in the following (layered) control on data transfers.

2.2.5 Assessment of the data transfer mechanism (if relevant)

Control	**Assessment of the adequacy of the transfer mechanism, declared by the CSP, based on the information provided during the onboarding process and/or in the contractual documents uploaded by the CSP, under Article 44-49 of the GDPR.**

	Note: if the service is only performed in the EEA, this control is not considered.
Type	Layered.
Question (for the legal expert)	What is the level of protection offered to the CSP's counterparty by the transfer mechanism offered by the CSP, taking into account available guidance on this point?
Possible answers	No protection (no actual proof of presence, clear non-compliance, unenforceability).
	Low protection (the transfer mechanism and related documents are faulty, provide a low level of protection, or are otherwise clearly less than ideal, but seem to be sufficiently conforming to the applicable law to not be an immediate compliance issue).
	Medium protection (the transfer mechanisms and related documents are adequately described, enforceable and provide a more or less balanced level of protection and obligations and rights).
	High protection (the transfer mechanism and related documents are adequately described, enforceable and provide a strong protection and rights for the application developer/target user organization as a controller).
Reason for inclusion	Data transfers have to be subject to adequate safeguards. This is a high compliance risk for the controller if not taken into account and therefore an essential point to include. It is included also as a layered control because of its importance, so as to avoid that CSPs simply declare to be in compliance, while the transfer mechanism and related documents provided are insufficient or not present.

2.2.6 Presence of a data processing agreement (DPA)

Control	**Presence of data processing agreement as defined in Article 28 GDPR and compliant with that Article offered by the CSP.**
Type	Simple.
Question	Do you provide a data processing agreement which is compliant with Article 28 of the GPDR?
Possible answers	Yes.
	No.

Reason for inclusion	A data processing agreement under Article 28 GDPR is again an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. Therefore, this is an essential control to include. It is included as a simple control by declaration of the CSP, as well as assessed in its contents through layered controls, as presented below.

2.2.7 Assessment of the scope of the DPA

Control	**Adequacy of the scope description in the DPA, as required by Article 28(3) GDPR.**
Type	Layered.
Question (for the legal expert)	How would you assess the description of subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects as required by Article 28(3) GDPR in the DPA under revision?
Possible answers	Description not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Therefore, this is an essential control to include.

2.2.8 Assessment of the obligation in the DPA for the CSP to only process data on the documented instructions of the CSP's counterparty

Control	**Adequacy of the contractual obligation for the CSP as a (sub-) processor to process personal data, including with regards to data transfers outside the EEA, only on the documented instructions of the CSP's counterparty, as prescribed by Article 28(3), a) GDPR, unless required to do so by EU or member state law, in which case the CSP has to inform its counterparty of that legal requirement, unless that in itself is forbidden by the legal rule in question.**
Type	Layered.
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP as a (sub-)processor to only act on the documented instructions of the CSP's counterparty, in the light of Article 28(3), a) of the GDPR and the current official interpretation available?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Therefore, this is an essential control to include. Having a clear contractual obligation to only process on the written instructions of the controller enables the controller to retain control. Anything outside this scope will lead to the CSP being qualified as a controller in its own right, with the consequent responsibilities.

2.2.9 Assessment of confidentiality obligations in the DPA for persons authorized to process data on behalf of the CSP

Control	**Adequacy of the contractual obligation for the CSP to ensure confidentiality of personnel and agents authorized to process data on its behalf through commitments of confidentiality or by the relevant persons being under a statutory obligation of confidentiality, as prescribed by Article 28(3), b) GDPR.**
Type	Layered.
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP to ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context, it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Therefore, this is an essential control to include. Sufficient obligations of confidentiality are essential measures to ensure that any personal data that a CSP and its personnel becomes privy of is not further divulged.

2.2.10 Assessment of the obligation in the DPA for the CSP to take all security measures pursuant to Article 32 GDPR

Control	**Adequacy of the contractual obligation for the CSP to take the appropriate technical and organizational measures to ensure a level of security appropriate to the risk, pursuant to Article 32 GDPR, as prescribed by Article 28(3), c) GDPR.**
Type	Layered.
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP to take all security measures pursuant to Article 32 GDPR, in the light of the obligation of Article 28(3), c) GDPR to include a clause detailing such measures in the DPA?
Possible answers	Obligation not present.
	Present, but potentially faulty (e.g. making the controller agree that a certain set of current measures will forever be appropriate) or unclear description given the context of the given CSP (reservation), so that it may be insufficient under Article 28(3), c) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), c) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Therefore, this is an essential control to include. While it is not possible for the legal expert to judge the adequacy of the concrete measures described by the CSP, the expert can assess the adequacy of the contractual guarantees.

2.2.11 Assessment of the obligations in the DPA in relation to initial sub-processor engagement by the CSP

Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the engagement of sub-processors by the CSP, specifically the need to have prior general or specific written authorization, and, in the case of general authorization, to inform its counterparty of intended changes, offering its counterparty an opportunity to object to such changes, as prescribed by Article 28(3), d) and 28(2) GDPR.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(2) GDPR, as referred to in Article 28(3), d) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonably short delays, an infeasible manner of objection, or other conditions arguably hollowing out the legally intended effect of Article 28(2) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Therefore, this is an essential control to include. Having a clear obligation on the engagement of sub-processors is a minimal requirement for the controller to retain a degree of control on the chain of processing of its data and the parties involved.

2.2.12 Assessment of the obligation in the DPA in relation to the contractual pushdown of data protection terms on a sub-processor of the CSP

Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the consequences of engaging a sub-processor, namely that the same data protection obligations binding the CSP to the CSP's counterparty should be passed down to the sub-processor of the CSP, as prescribed by Article 28(3), d) GDPR and Article 28(4) GDPR.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with the requirement of pushing down the same data protection terms binding the CSP on any sub-processors engaged in the processing by the CSP, as described in Article 28(4) GDPR, as referred to in Article 28(3), d) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential limitations or obscurity created by the contract terms which may be interpreted as such, arguably hollowing out the legally intended effect of Article 28(4) GDPR. (Low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	As explained before, in a multi-Cloud context it is very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Therefore, this is an essential control to include. Having sub-processors be bound by the same data protection terms ensures that they respect the spirit of the agreement between the controller and the CSP as a first processor. Note that when the CSP is not a first processor , the same terms will need to pushed up instead by the application developer, who will become the first processor, in order to meet the requirements that throughout the chain of processing, the data protection terms are the same (or equivalent).

2.2.13 Assessment of the obligation in the DPA stating that the CSP remains liable for a sub-processor's failures to fulfil its obligations

Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the consequences of engaging a sub-processor, namely that there should be a clear affirmation that the CSP shall in any case remain liable towards the CSP's counterparty for failure of its sub-processor to perform its obligations, as prescribed by Article 28(3), d) GDPR and Article 28(4) GDPR.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(4) GDPR, as referred to in Article 28(3), d) GDPR, namely that there should be a clear statement that the CSP will always remain liable towards its counterparty if the CSPs sub-processor fails to fulfil its obligations?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential limitations or obscurity created by the contract terms which may be interpreted as such, arguably hollowing out the legally intended effect of Article 28(4) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	As explained before, in a multi-Cloud context it is very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. CSP liability serves as a back-up mechanism in case the sub-processor would fail to fulfil its obligations, putting pressure on the CSP to select only reliable sub-processors. This is especially important for the application developer when the application developer's organization becomes the first processor and its client(s) the controller.

2.2.14 Assessment of the obligation contained in the DPA for the CSP to take the necessary measures to assist its counterparty with data subject requests

Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the CSP assisting its counterparty, by appropriate technical and operational measures insofar as this is possible, to respond to data subject requests, as prescribed by Article 28(3), e) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including those relating to cost and conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(3), e) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of high costs, unreasonable conditions or other, arguably hollowing out the legally intended effect of Article 28(3), e) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), e) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. While it is primarily the controller who needs to deal with data subject requests, assistance by processors may be necessary at times for technical or organizational reasons. There should be a clear obligation on this and any remuneration to the CSP should be reasonable.

2.2.15 Assessment of the obligation contained in the DPA for the CSP to support its counterparty with its own obligation to ensure security of processing (Article 32 GDPR)

Control	**This control relates to the adequacy of the contractual obligation in the DPA with regards to the CSP's obligation to assist its counterparty in attaining an adequate level of security of processing as meant in Article 32 GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including those relating to cost and conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide assistance to its counterparty in the counterparty's own obligation to ensure an adequate level of security of processing, as required by Article 28(3), f) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of high costs, unreasonable conditions or other, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Next to the CSP's own obligation to take the necessary measures pursuant to Article 32 GDPR (as required by Article 28(3), c) GDPR), Article 28(3), f) also requires there to be a clear obligation for the CSP to help its counterparty take such measures, where the nature of the processing and the information available to the processor allows this.

2.2.16 Assessment of the obligation contained in the DPA for the CSP to support its counterparty with data breach notifications to the supervisory authority and/or the data subject

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to support its counterparty with the latter's obligation to notify the supervisory authority and/or the data subject in case of a data breach, likely to result in a (high) risk for data subjects, as provided in Article 28(3), f) GDPR, 33 GDPR and 34 GDPR. It assesses the content of that obligation in the DPA and its potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide support in fulfilling the notification obligations of Article 33 and 34 GDPR as required by Article 28(3), f) GDPR, specifically outside the own processor-specific obligation to notify the controller without undue delay after becoming aware of a data breach (Article 33(2) GDPR)?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Assistance by the CSP in a situation of a personal data breach can be essential for the CSP's counterparty to fulfil its obligations in a correct a timely manner, avoiding (further) compliance issues. This presupposes clear contractual terms on top of Article 33(2) GDPR providing for a clear processor-specific obligation to notify its counterparty without undue delay.

2.2.17 Assessment of the obligation contained in the DPA for the CSP to support its counterparty with data protection impact assessments (DPIAs) and, where applicable, prior consultation with the supervisory authority

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to support its counterparty with the latter's obligation to carry out a data protection impact assessment (DPIA) on intended processing activities that meet the requirements set by Article 35 GDPR (likely to result in a high risk for the data subject) and to consult with a supervisory authority prior to carrying out the planned processing activity when the outcome of the data protection impact assessment is that there is a high residual risk, despite the risk containment and prevention measures already taken by the counterparty and detailed in the DPIA, i.e. that there is a high risk remaining in the absence of further controlling measures to be taken by the controller (Article 36 GDPR). It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide support in fulfilling its counterparty's obligation to carry out a data protection impact assessment under the conditions provide in Article 35 GDPR and, where applicable, of the prior consultation obligation contained in Article 36 GDPR, as required by Article 28(3), f) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, unreasonably high costs, lack of capacity of the counterparty to decide when a data protection impact assessment or prior consultation is necessary, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud

	context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Assistance by the CSP in carrying out a data protection impact assessment may be vital in determining some of the technical and organizational security measures of the intended processing, which have a clear impact on the residual risk that must be identified, on the basis of which the controller has to make the important and legally very relevant decision to go ahead with the intended risky processing or not. It is therefore very important that the controller is guaranteed in a non-preventative way that the CSP will cooperate with such activities. The same is true for the situation in which the data protection impact assessment has revealed that there is still a high residual risk to be addressed through a prior consultation with a supervisory authority. Here as well, to assess what can be done and whether the processing can in then end be carried out (e.g. with added security measures), the CSPs input can be very relevant. It is important to have clear obligations on this matter, without the CSP being able to hollow out this obligation, e.g. because of contractual terms enabling it to refuse in certain cases, charge unreasonably or preventatively high costs for this assistance etc.

2.2.18 Assessment of the obligation in the DPA for the CSP to delete or return (at the choice of its counterparty) all personal data at the end of the contract

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to delete or return, at the choice of its counterparty, all personal data of the controller at the end of the contract, unless EU or member state law specifically requires further storage of that data, as defined in Article 28(3), g) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to, a the choice of the counterparty, delete or return all personal data to the counterparty at the end of the provision of services?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably

	hollowing out the legally intended effect of Article 28(3), g) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), g) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. The principal obligation for the CSP to get rid of the data at the end of the contract is vital for the CSP's counterparty to ensure its data does not start leading a second life outside its control, leading to a range of potential issues.

2.2.19 Assessment of the obligation in the DPA for the CSP to provide its counterparty with all information necessary to demonstrate compliance

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to provide its counterparty with all compliance information necessary, specifically to show the CSP's compliance with the obligations defined by Article 28, as defined in Article 28(3), h) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP to make available to its counterparty all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), h) GDPR (low protection).

	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), h) GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Having a clear obligation with little restrictions to obtain all necessary compliance information from the CSP as a processor is an elementary part of the controller's responsibility to monitor its processors, in application of its obligation to only engage processor providing sufficient guarantees not only in the contract, but also in reality. This is important for the counterparty whether or not it acts as a controller or a processor, since in the latter case, that obligation will rest with the counterparty's client.

2.2.20 Assessment of the obligation in the DPA for the CSP to allow for and contribute to audits, including inspections, conducted by the counterparty or another auditor mandated by the counterparty

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to allow for and contribute to audits, including inspections either carried out by the counterparty itself or by another auditor mandated by the counterparty, as required explicitly by Article 28(3), h) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Type	Layered.
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP submit itself to audits, including inspections carried out by the counterparty itself or by another auditor mandated by the counterparty, as required by Article 28(3), h) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions (high costs, long delays, etc.),

	carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), h) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), h) GDPR (medium protection).
	Present and fully adequate, providing for real audit and inspection rights at reasonable conditions for the counterparty (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. Having a clear obligation with little restrictions to audit the CSP gives the counterparty a strong measure of control to verify statements and claims by the CSP. It is an instrument of importance, although the CSP may want to try and limit this right. Therefore, this is very relevant to the legal level a CSP is offering for a given service.

2.2.21 Assessment of the obligation in the DPA for the CSP to immediately inform its counterparty if, in the CSP's opinion, an instruction infringes applicable data protection law

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to immediately inform the counterparty if any of its instructions are, in the opinion of the CSP, contrary to applicable data protection law (GDPR, EU law or member state law).**
Type	Layered.
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP to immediately inform the counterparty if it considers any of the counterparty's instructions contrary to applicable data protection law as required by Article 28(3), second subparagraph GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential delays, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), second subparagraph GDPR (low protection).

	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), second subparagraph GDPR (medium protection).
	Present and fully adequate (high protection).
Reason for inclusion	A data processing agreement under Article 28 GDPR is an essential measure to be present. The controller (typically the target user organization) has a strict obligation to have such a contract with processors, such as the CSP. It is a necessary and suitable instrument to provide compliance with the obligation under Article 28(1) GDPR to only use processors which provide sufficient guarantees. In a multi-Cloud context it is therefore very important to ensure that data processing agreements with all CSPs used are in full compliance with Article 28(3) of the GDPR to avoid compliance issues. Such a contract has to conform to all aspects of Article 28(3) of the GDPR. Non-compliance with one aspect can be sufficient to have compliance issues. A clear obligation for the CSP to immediately inform the counterparty of faulty processing instructions, which are contrary to applicable data protection law is an important mechanism to ensure that CSPs do not blindly follow instructions and put responsibility with the counterparty, but actively engage in a legal analysis of the situations the are confronted with as well.

2.2.22 Assessment of liability clauses under the DPA (if relevant)

Control	**This control aims to assess the liability clause in the DPA, if any are present, even by reference to other contractual documents. Liability clauses in the DPA specifically may be different from the general liability clause, and have to be in accordance with Article 82 GDPR.** **The control looks at all liability clauses for data protection matters, including liability towards data subjects, liability for fines and related matters of liability. The full liability for sub-processors that the CSP has to guarantee under Article 28 can also be relevant here, since that Article requires "full liability". Thus a statement in the previous control of full liability could be curtailed by a limiting liability clause.** **Note: If no clause is present, this control is not considered, since it cannot in general terms be stated whether or not this is a positive or a negative point.**
Type	Layered.
Question (for the legal expert)	How do you assess the liability situation for data protection related matters (liability towards data subjects, for fines, for related matters, full liability of the processor for the sub-processor) under the DPA, especially

	in the light of Article 82 GDPR and taking into account the impact of that Article on the principal freedom of contract of the Parties?
Possible answers	Exclusions are present in a wording clearly in direct conflict of the GDPR, e.g. conflicting with the terms of Article 82 GDPR or providing for backdoor circumvention of Article 28(4) GDPR.
	The DPA contains some clear liability caps, limitations and/or exclusions, the text of which may be in conflict with the GDPR and/or are very negative for the counterparty (reservation) (low protection).
	The DPA contains liability caps, limitations and/or exclusions, the text of which is likely compliant with the GDPR and provides at least a reasonable measure of balance between the contracting parties (medium protection)
	The DPA contains liability caps, limitations and/or exclusions which are balanced and clearly within the margin of appreciation of the parties, not depriving the contract of its essence (high protection).
Reason for inclusion	Liability for data protection related matters is evidently an important topic for Cloud users (i.e. the target organizations), given the potential huge financial impact of the GDPR, both in terms of potential litigation for data subject rights and because of the potential large fines that may be imposed by supervising authorities. Clear and balanced obligations, a lack of unreasonable caps or other exclusions, etc. can both ensure compliance with the GDPR and help avoid discussions afterwards.

2.2.23 Assessment of termination clause under the DPA (if relevant)

Control	**This control addresses the termination clause of the DPA, if there is any. Such a clause is not obligatory but if present must not limit the effect of the DPA. In practice such clauses are nonetheless found and they have the effect of hollowing out the intended effect of article 28 GDPR. This control aims to assess this potential threat.** **Note: If no clause is present, this control is not considered, since it cannot in general terms be stated whether or not this is a positive or a negative point.**
Type	Layered.
Question (for the legal expert)	If there is a termination clause in the DPA, does it ensure protection of the CSP's counterparty and compliance under article 28 GDPR?
Possible answers	No, the DPA can easily be terminated, leaving the service contract of the services that contain the processing activities intact, without a valid DPA.
	This is unclear, the wording of the contract is vague or faulty, or there is a reference which does not contain specific language on this topic; it could

	reasonably be questioned whether this clause has the effect of hollowing out Article 28 GDPR (reservation) low protection.
	The DPA's termination clause is reasonably formulated and to be interpreted as logically following the main service agreement; it is unlikely to be interpreted as hollowing out Article 28 GDPR (medium protection).
	The DPA's termination clause is clearly worded and leaves no or little room for misinterpretation. The DPA logically follows the main contract. It is very likely compliant with the GDPR and does not hollow out Article 28 GDPR (high protection).
Reason for inclusion	While this may seem obvious, even a fully compliant processing agreement under Article 28 GDPR would lose a sizeable part of its effect and compliance benefits if there were to be a termination clause that undercuts the intended effect of Article 28 GDPR by making a termination possible while the related service agreement and the provision of services are maintained. Thus, if any clauses are present, whether or not by reference to other contractual documents, it is extremely relevant to ensure that those termination terms, their conditions and the timing is a match to ensure that Article 28 GDPR is respected throughout the whole duration of the provision of services.

2.2.24 Assessment of the contractual terms on alternative dispute resolution mechanisms (if relevant)

Control	**This control aims to assess the content of the alternative dispute resolution clause, if any is present, in order to ensure that the clause is both enforceable and useful, i.e. not subject to prohibitive conditions or conditions/exceptions that render it ineffective. In addition, it aims to ensure that the ADR options are available to the CSP's counterparty, but not force upon it, as it may be preferable for the CSP's counterparty not to have to submit to ADR mechanisms, such as arbitration.**
Type	Layered.
Question (for the legal expert)	Examining the content of the alternative dispute resolution clause, what level of protection does it offer to the CSP's counterparty, taking into account that an alternative dispute resolution clause should be enforceable and not subject to limitations and/or conditions that are prohibitive or render it ineffective, nor should it be the only binding option, as, depending on the situation the CSP's counterparty may prefer not to take the ADR route?
Possible answers	There are clear compliance issues (contra legem wording), serious prohibitive conditions or carveouts, or there are other issues that render the clause either impossible to be executed, ineffective, or otherwise useless to the CSP's counterparty.

	The clause is enforceable and effective, but the conditions or exclusions make it unlikely to be used in reality or it makes ADR binding without any other options being available, effectively forcing e.g. expensive arbitration on the CSP's counterparty (reservation) (low protection).
	The clause is enforceable and effective, effective use may reasonably depend on the situation, while it remains possible to go to court (medium protection).
	The clause is enforceable and effective and motivating for the CSPs counterparty to use the mechanisms offered, while in no way forcing such. There are satisfactory back-up mechanisms for the CSP's counterparty, e.g. there is a right to request mediation but going to court instead or afterwards remains possible (high protection).
Reason for inclusion	While the value of this lies in the eye of the beholder, alternative dispute resolution mechanisms like arbitration, binding third party decision, reconciliation, mediation etc. can be a valuable provision in a contract. For EU customers, litigation in the USA or other third countries can prove prohibitively costly, difficult or outright ineffective. Alternative dispute resolution mechanisms may do better and alleviate some of the concerns of traditional litigation. Hence the inclusion as a relevant control for some of the target organizations. Nonetheless, the specific wording and conditions of such mechanisms is relevant to consider. Some wordings may be contrary to applicable law or clearly unenforceable. Others may be faulty and the possibility to rely on them may be uncertain. Next to enforceability, the conditions attached to these mechanisms may be prohibitive or render them ineffective. Therefore, it is necessary to also assess the content of such terms. Moreover, while ADR may be a useful manner in which to deal with conflicts, some Cloud users may prefer not to be bound by such a mechanism. For example, a binding arbitration clause forcing the parties into a potentially expensive arbitration, which can moreover not be appealed. Thus it is important to also include this language in the control. Therefore, this layered control should be included.

2.2.25 Assessment of the contractual terms on termination of the contract with regards to the ease with which the CSP's counterparty can terminate the contract

Control	**This control assesses the level of the contractual possibilities to terminate the contract with the CSP. It aims to measure how flexibly the counterparty of the CSP can get out of the contract. Some termination possibilities are standard, e.g. for material breach. Others are not. Some CSPs offer very flexibly terminated contracts, while others strictly limit this, through a variety of clauses, including through the manner in which**

	notification can be given. The consequences of termination are also taking into account.
Type	Layered.
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms, how do you assess the level of ease offered to the CSP's counterparty in terminating the contract in a situation where the CSP's services are no longer wanted, also taking account of any consequences of termination?
Possible answers	There are unreasonable punitive clauses, limitations and exceptions or otherwise clauses which make termination very difficult.
	Termination is possible, but only in limited circumstances e.g. breach of contract, or with a very early prior notice, or under conditions which are substantially aimed to protect the CSP (reservation) (low protection)
	Termination is possible in most or all circumstances, notice periods are reasonable if any and the conditions are reasonably balanced, termination is also possible without notice under breach of contract, although grace periods may apply. (medium protection)
	Termination is very easy and always possible. No notice period applies or it is very limited. Breach of contract justifies immediate termination with little grace periods, if any. All conditions are favourable to the CSP's counterparty (high protection).
Reason for inclusion	While DECIDE will enable different combinations of contractual relationships with the Cloud Service Provider (own credentials, credentials through ACSmI where ACSmI has a contract with the CSP), there will be several scenarios in which the DECIDE user (i.e. the application developer's organization) will have a direct contract with the CSP. In a multi-Cloud setting, a certain CSP may over time become obsolete. In such a case, it is arguably a positive factor to be able to terminate the contract with the CSP flexibly, without punitive clauses or far-going limitations.

2.2.26 Assessment of the contractual terms on termination of the contract with regards to the options available to the CSP to terminate or suspend the contract

Control	**This control assesses the options available to the CSP to terminate or suspend the contract and the resulting level of protection of the CSP's counterparty in continuity of the enlisted services.**
Type	Layered.

Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms, how do you assess the level of protection offered to the CSP's counterparty when looking at the options available to the CSP to terminate or suspend the contract.
Possible answers	There is no protection. The CSP can terminate and/or suspend at will, with no reason or notice and there are no mechanisms to ease the transition.
	Termination and/or suspension is very easy for the CSP, many options being available with a low threshold, including options for termination/suspension without notice based on very low-threshold contractual shortcomings of the counterparty (reservation) (low protection)
	Termination and/or suspension are possible in several circumstances, but there are notice periods and/or other mechanisms to ease transition and this is reasonable. Termination/suspension without notice is only possible on the basis of reasonable conditions (medium protection).
	Termination and/or suspension are possible in a reasonably limited number of circumstances. Notice periods and/or other mechanisms to ease transition are favourable to the CSP's counterparty. Termination/suspension without notice is strictly limited (high protection).
Reason for inclusion	Whether the contract is directly concluded with the application developer or target user organization or with ACSmI as an intermediary, it is always important for reasons of continuity that the enlisted Cloud services can be depended on to remain available. Of course termination by the CSP will always be possible in certain circumstances (e.g. when the user doesn't pay), but it is important that the termination and/or suspension possibilities of the CSP are not too protective, leaving the CSP's counterparty, and in the end effectively the DECIDE user, with little certainty. And while multi-Cloud in DECIDE is inherently meant to be dynamic, a measure of continuity and reliability in legal terms nonetheless holds value. Hence the inclusion in the legal level for the consideration of the application developer and/or target user organization of the multi-Cloud application in question.

2.2.27 Assessment of the contractual terms on changes to the contractual documents with regards to the level of protection offered to the CSP's counterparty from potentially disruptive unilateral changes of contract

Control	**This control assesses whether or not, and to what extent the CSP is reserving the right to unilaterally change the contractual documents. This is a provision often found in CSP contracts and may be an issues if the changed terms are unacceptable for the user. The way in which this is done and the period of notice are relevant factors to take into account. The control is measuring the level of protection for the CSP's**

	counterparty, and thus more flexibility for the CSP means less protection in terms of guaranteed continuity for the CSP's counterparty. The absence of such a clause, which implies that the contract is permanent and more durable, is a positive point. In a way, this is the other side of the coin of the control on ease of termination for the CSP's counterparty.
Type	Layered.
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms how do you assess the level of protection offered to the CSP's counterparty from potentially disruptive unilateral changes of contract?
Possible answers	Unilateral changes are possible, without the CSP having to give a reason, and with very little to no notice period, giving the CSP's counterparty little to no time to find alternatives if the new terms are unsuitable.
	Unilateral changes are possible, without the CSP having to give a reason, and with a short notice period, giving the CSP's counterparty some opportunity to find alternative solutions if the new terms of the contract are unsuitable (reservation) (low protection).
	Unilateral changes are possible, with or without the CSP having to give a reason, but there is a reasonable notice period and potentially other mechanisms giving the CSP's counterparty a fair opportunity to find alternative solutions if the new terms of the contract are unsuitable (medium protection).
	Unilateral changes are not possible. The contract is fixed for its duration in its terms (high protection).
Reason for inclusion	This control assesses how easy it is (or if at all possible) for the CSP to unilaterally change the contract. This may be very relevant for DECIDE users both when contracting directly with the CSP or through ACSmI as an intermediary. If the terms of the contract are changed unilaterally by the CSP, the service may no longer be suitable for the application based on the legal needs of the target user organization. Thus, this may disrupt the continuity of the deployment of the multi-Cloud application, certainly if there is little notice period and no reasonable alternatives are readily available. Hence, this is likely a relevant control to take into account when assessing the legal level.

2.2.28 Assessment of the general contractual terms on liability and the limitation thereof

Control	**This control relates to the terms in the contractual documents provided by the CSP in relation to the determination of liability, and, specifically**

	the limitations of liability that are present, looking at the level of protection offered to the CSP's counterparty.
Type	Layered.
Question (for the legal expert)	Taking into account all terms in the contractual documents, what is the level of protection offered to the CSP's counterparty in terms of options to recover damages, taking into account the extent to which liability is limited?
Possible answers	There is no option. All liability is excluded, even contra legem.
	There are theoretical options to recover damages but they are heavily limited and it is questionable that in reality the CSP's counterparty will be able to obtain a reasonable measure of redress, e.g. because of far-reaching carve-outs or a very restrictive liability cap (reservation) (low protection).
	There are options to recover damages, although limited in a reasonable way and according to industry practice. Redress is reasonably obtainable but may be limited in amount (medium protection)
	There are reasonable and balanced options to recover damages. Limitations are either not present or favourable for the CSP's counterparty (high protection).
Reason for inclusion	While liability is often severely limited in CSP contracts and while it may not be the main concern of many Cloud customers, it may nonetheless be a legally relevant aspect to take into account. If a CSP were to cover above average options, this should be indicated and stand out, hence the inclusion of this control.

2.2.29 Assessment of contractual terms relating to force majeure

Control	**This control relates to the contractual definition of force majeure, which prevents any liability from arising at all. The conditions under which force majeure is considered to be present may be another way for the CSP to limit it's liability towards the counterparty.**
Type	Layered.
Question (for the legal expert)	Taking into account the contractual terms on force majeure, how do you assess the remaining level of protection for the CSP's counterparty, taking into account that, while force majeure is a reasonable exception in itself, an overly extensive interpretation may create a backdoor for the CSP to unduly escape liability?

Possible answers	Force majeure is interpreted so extensively that no liability can ever exist.
	Force majeure has a (very) extensive interpretation, posing a real risk of hollowing out any liability possibility, which will likely lead to discussion if certain events arise (reservation) (low protection).
	Force majeure is described in a reasonable manner and does not principally hollow out liability (medium protection)
	Force majeure is described clearly and precisely and is limited to classic force majeure scenarios (high protection).
Reason for inclusion	Clauses on force majeure are added as a control for the same reason as liability itself. The measure in which damages may be recovered in case something goes terribly wrong is definitely a legally relevant aspect. While limitations of liability may be one way for the CSP to avoid to have to pay for the counterparty's redress in case of damages, force majeure may be just as effective. For this reason, it should be included as a control and measured that the provisions do not lead to excluding any liability whatsoever, outside the accepted concept in legal theory of force majeure.

2.2.30 Assessment of general contractual terms on confidentiality

Control	**This control relates to the contractual provisions on confidentiality, other than the confidentiality obligations under Article 28 GDPR, but rather in more general terms.** **The focus of the control is first on the fact that confidentiality should be comprehensive and the obligation clear and enforceable. Typically, confidentiality applies to both Parties equally, but if not, the focus would be on the CSP's part of the obligation.**
Type	Layered.
Question (for the legal expert)	What is the level of protection offered by the text of the general confidentiality obligations resting on the parties, specifically on the CSP?
Possible answers	No confidentiality is guaranteed.
	Basic references are available to confidentiality but faulty and/or incomprehensive, and/or enforcement problems to be expected (reservation) (low protection).
	There is a clear and enforceable confidentiality obligation for both Parties (medium protection).

	Confidentiality obligations are clear and enforceable and are fully comprehensive (high protection).
Reason for inclusion	General confidentiality obligations can have an important impact on business as it prevents sensitive information from being divulged. Thus, it is legally relevant to assess the contractual terms on this and specifically the level of confidentiality the CSP commits to. This is a much broader obligation than the confidentiality mentioned above under the data processing agreement and should therefore be treated separately.

2.2.31 Presence of ISO 27001 certification or equivalent covering the service

Control	**This control aims to verify whether the service in question offered by the CSP is certified under ISO 27001 or equivalent certification standards providing a level of information security management practices at the CSP.**
Type	Simple
Question	Did your organization obtain and does it maintain a certification under the ISO 27001 standard or equivalent, covering the service in question that is less than 3 years old in its current form and proof of which is available to the customer upon request?
Possible answers	Yes.
	No.
Reason for inclusion	ISO 27001 and equivalent certifications of a CSP and the service offered show that a given amount of information security management controls are in place, as defined in the relevant standard. While not specific to Cloud services or CSPs, this is may be a valuable indicator of a base level of information security, which a Cloud customer may reasonably expect to be present at the CSP and for the given service, given that the move to Cloud inescapably involves a measure of control being released by the controller over the information that is processed in the Cloud. Certifications can be a practical means of ascertaining to what extent the information will be safe with the CSP.

2.2.32 Presence of Cloud-specific certification that meets all CCSM security objectives

Control	**This control aims to verify whether the service in question offered by the CSP is certified under a certification that meets all of the 27 security objectives of the Cloud Certification Schemes Metaframework as defined by ENISA. Examples include CSA attestation/certification – OCF level 2 and TÜV Rheinland Certified Cloud Service certification.**

Type	Simple
Question	Did your organization obtain and does it maintain at least one certification that meets all of the 27 security objectives of the Cloud Certification Schemes Metaframework as defined by ENISA, such as CSA attestation/certification – OCF level 2, TÜV Rheinland Certified Cloud Service certification or equivalent, which covers the service in question, is less than 3 years old in its current form and proof of which is available to the customer upon request?
Possible answers	Yes.
	No.
Reason for inclusion	In its 2014 paper [3], ENISA defined 27 security objectives for measuring the security level of a CSP and services offered and mapped this against existing certifications. Several Cloud-specific certifications touch upon all of these objectives. The presence of at least one such certification can be a useful indicator of the level of security present at the CSP, covering the Cloud service in question.

2.2.33 Presence of adherence to a Code of Conduct for Data Portability and Cloud Service Switching

Control	**This control relates to the adherence of the CSP to a self-regulatory instrument (code of conduct) setting reasonable industry standards for data portability and switching as intended by Article 6 the Regulation on the free flow of data** [4]**.**
Type	Simple
Question	Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting reasonable industry standards for data portability and switching as intended by Article 6 of the Regulation on the free flow of data?
Possible answers	Yes.
	No.
Reason for inclusion	This control responds to Article 6 of the Regulation on the free flow of data [4], which proposes self-regulation through codes of conduct for the issues of data porting. Adherence to such a code of conduct shows are clear commitment to providing easy and useful portability and switching options, as well as a general compliance commitment. Adherence also provides a certain guarantee that measures are in place. This all benefits the Cloud user who

	may want to switch providers, a very real and pertinent scenario in a multi-Cloud environment. Adherence to such a code is therefore of great importance for a target organization choosing a CSP. While at the time of writing only this white paper the SWIPO IAAS Code of Conduct [5]is at a mature stage, it can be envisioned that this control will at least correlate to one existing code of conduct by the time DECIDE is put into practice. In any case this Code of Conduct is most relevant to DECIDE, which has a sole focus on IaaS.

2.2.34 Presence of adherence to a Data Protection Code of Conduct for Cloud Service Providers

Control	**This control relates to the adherence of the CSP to a self-regulatory instrument (code of conduct) relating to data protection, which has been approved under Article 40 GDPR.**
Type	Simple
Question	Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting out data protection requirements, approved under Article 40 GDPR?
Possible answers	Yes.
	No.
Reason for inclusion	Article 28(5) GDPR especially mentions codes of conduct approved under Article 40 GDPR as a good means to check whether a CSP is able to provide sufficient safeguards to be employed as a processor. It may even serve to identify suitable sub-processors. While such adherence cannot replace any other assessment by the controller/target user organization, it can be a very useful element, hence the inclusion in the legal level. First of course, such codes of conduct have to be written and approved. At the time of writing, this has not happened yet, but it can be expected that by the time DECIDE will be operational, such approved codes will exist. If not, this control we need to be adapted to reflect that reality. Two examples of existing codes are: first, the EU cloud code of conduct developed by the Cloud Select Industry Group in close cooperation with the European data protection regulatory bodies [6] and second, the CISPE code of conduct [7].These codes of conduct should allow the CSP to establish which requirements they should meet under the GDPR, the assurances they already have from existing certifications, and how they can fill the remaining gaps, leading to an acceptance of adherence if they manage to fill the gaps. For a code to have comprehensive value, it should be approved under Article 40 GDPR.

	This control may need to be updated along the way, as it may be the case that the codes of conduct will itself institute different levels of adherence/compliance (e.g. self-assessed, verified, certified) and different levels of monitoring and enforcement may be present, leading to a need to differentiate this control further. .

2.3 General considerations with regards to the legal controls

Two important elements need to be noted in this section:

- The way in which controls function (verified layered controls vs. self-declared simple controls) and;
- The justification for the inclusion of some legally relevant aspects as controls and the exclusion of others.

They are discussed in turn in the following subsections.

2.3.1 Considerations with regards to the way in which controls function

The controls described in section 2.2 and its subsections above are based on a combination of legally relevant aspects that can be ascertained through a contract review (as the CSP will have to upload its contractual documents) by a legal expert and a series of questions on legally relevant that have to be answered by the CSP because they cannot be assessed on the basis of the contractual terms.

Thus, it combines an approach of verification of the level of certain legally relevant aspects (through layered controls, i.e. by reviewing and assessing the contractual terms) with an approach of mere declaration of certain other legally relevant aspects by the CSP (through simple controls, translated into direct yes/no questions to the CSP). These declarations are however made binding through the contractual framework binding the CSP to DECIDE as described in section and consequently can be relied upon by the DECIDE user.

The aspects covered by declaration in this way are the following:

Table 4. Questions for the CSP (simple controls)

Control	Question to the CSP
Valid company registration	Is your organization a validly registered and incorporated entity, which is neither in liquidation nor in a state of bankruptcy?
Presence of a DPO/data protection point of contact	Did your organization appoint and will it maintain a DPO in accordance with Articles 37-39 of the GDPR or an equivalent position e.g. a privacy officer or privacy team which can act as a data protection point of contact?
Presence of a representative in the EU (if relevant)	Did your organization appoint and will it maintain a representative in accordance with Article 27 of the GDPR?
Presence of a data transfer mechanism declared by the CSP (if relevant)	In case data is transferred outside the EEA, do you have in place sufficient safeguards, as described in Articles 44-49 of the GDPR?
Presence of a data processing agreement (DPA)	Do you provide a data processing agreement which is compliant with Article 28 of the GPDR?

Presence of ISO 27001 certification or equivalent covering the service	Did your organization obtain and does it maintain a certification under the ISO 27001 standard or equivalent, covering the service in question that is less than 3 years old in its current form and proof of which is available to the customer upon request?
Presence of Cloud-specific certification that meets all CCSM security objectives	Did your organization obtain and does it maintain at least one certification that meets all of the 27 security objectives of the Cloud Certification Schemes Metaframework as defined by ENISA, such as CSA attestation/certification – OCF level 2, TÜV Rheinland Certified Cloud Service certification or equivalent, which covers the service in question, is less than 3 years old in its current form and proof of which is available to the customer upon request?
Presence of adherence to a Code of Conduct for Data Portability and Cloud Service Switching	Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting reasonable industry standards for data portability and switching as intended by Article 6 of the Regulation on the free flow of data?
Presence of adherence to a Data Protection Code of Conduct for Cloud Service Providers	Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting out data protection requirements, approved under Article 40 GDPR?

This combination provides a cost-efficient, yet effective way to assign a meaningful legal level to any Cloud service. It goes further than mere declaration of all aspects by the CSP itself and is therefore more reliable. Only those aspects which are difficult to ascertain and for which the necessary information lies with the CSP are dealt with as simple controls.

Simple controls to be answered by the legal expert were avoided to avoid bias and/or mistakes based on lack of information. Layered controls to be answered by the CSP would evidently be useless as the CSP would be strongly biased towards giving itself a good score.

This manner is in no way the only one to assign a legal level to a Cloud service. For an outlook on what could be possible in the future to get to an even more reliable and valuable result, please refer to section 5 Sustainability and upscaling.

2.3.2 Considerations regarding the inclusion the justification for the inclusion of some legally relevant aspects as controls and the exclusion of others

As the described in deliverable D5.3, the legal level was to include at least the following aspects, their importance based on the law, existing contractual documents of CSPs accessible online, practical input by project partners and clear business importance:

- GDPR safeguards for data transfers if relevant
- GDPR compliance of data processing agreement with article 28 GDPR
- Presence of a representative in the EU and/or DPO, if relevant
- Applicable law and conflict resolution clauses

- Liability level (caps) and liability clauses
- Exit clauses and penalties (mostly to exclude services that prevent dynamic contracting by imposing penalties)
- Data portability and Cloud switching clauses

The legal level includes all these aspects in the form of controls mentioned above, and more.

However, there were other aspects which might have been included, but were not, for specific reasons, although they may have legal relevance and/or business relevance.

The following table clarifies why certain aspects/clauses were not retained:

Table 5. Potential legal controls that were not retained in the legal level

Legally relevant aspect	Reason for non-inclusion as a control
Determination in the contract of applicable law.	While legally relevant, preference on this depends on the very specific situation of the Cloud user. There is no abstract generic value to be assigned to one system of law or another being applicable. Thus, it would not be a useful control for the general DECIDE user.
Disclaimer and indemnity clauses in the contractual documents.	While not legally irrelevant, these are typically very broad standard clauses which are remarkably similar in most CSP contracts. It may be hard to differentiate between this further than presence or absence of the clause and is hard to assign a value to. This does also not represent a major risk or consideration in Cloud use.
SLA terms	While the SLA is part of the contractual documents and the controls need to be mapped against all contractual documents, including the SLA, there is no control specifically looking at the SLA of the service. This is because relevant content (e.g. availability) of the SLA is captured elsewhere in DECIDE. The relevance to the legal level of the Cloud service is minimal or non-existent, although the SLA is checked for the eventuality that some of its terms might have a legal implication/impact that is relevant to other controls.
Clauses on official notification (outdated)	Some CSP contracts contain remarkably outdated ways of giving the CSP official notice (fax, post). While this is relevant as such, it is covered under the legal control relating to termination options for the CSP's counterpart. This is because, while some CSP contracts provide for such methods, in practice there are other options to give notice and complete actions in the UI offered by the CSP. Thus, such contractual references may be merely a safety net. The detrimental value of such clauses is therefore unsure. Any language in the contract making notification (specifically termination)

Legally relevant aspect	Reason for non-inclusion as a control
	unworkable will in any case be caught under the aforementioned control.
Customer obligation clauses	Depending on the CSP involved and the type of Cloud service offered (bespoke vs. generic), very diverse clauses of customer obligations can be found, ranging from payment obligations and conditions to obligations in providing information, giving notice for certain events, rules on balancing and credits etc. These obligations depend on the relationship at issue and are too diverse and situation dependent to compare. Often, they are caught by other aspects of DECIDE and/or other legal controls. Bear in mind that the legal expert will always look at the entirety of the contract when assessing the controls. Language that is detrimental to the Cloud user will therefore be caught under other controls, e.g. language giving the CSP a myriad of reasons to suspend the Service if customer does not fulfil certain (far-going, unreasonable) obligations, is caught under the control "Assessment of the contractual terms on changes to the contractual documents with regards to the level of protection offered to the CSP's counterparty from potentially disruptive unilateral changes of contract". It could have been envisioned to add a general control on customer obligations as a catch-all, but the added value of this would be limited as it would entail an excessive leeway for the legal expert.
Diverse legal boilerplate	There are often indeed diverse other stipulations in the contractual documents, which, by themselves do not bear enough relevance in the multi-Cloud scenario to be included as a control of their own. It would have been possible to add a general control on as a catch-all to cover this language, but the added value of this would be limited as it would entail an excessive leeway for the legal expert. Moreover, as the legal expert will always look at the entirety of the contract when assessing the controls, language that is detrimental to the Cloud user under any of the other controls will be caught through those controls.
Other certification requirements	As described in deliverable D5.3 it is not possible to attach abstract value to the myriad of certifications that exist. The value is to an extent in the eyes of the beholder, although different certification schemes objectively have a different scope [8].Determining which certifications are right for a given

Legally relevant aspect	Reason for non-inclusion as a control
	DECIDE user may be an added value service provided by DECIDE partners as a stand-alone service. This is referenced in the DECIDE business plans. Therefore, it was decided to only include basic ISO 27001 (or equivalent) and a more substantive Cloud-specific certification (such as CSA attestation/certification – OCF level 2 or equivalent) as controls in the legal level, because these are quite standard and well-known. This may be changed and updated in the future to include certification schemes as they become available and/or more common on the market EU-wide. Examples could be the EU cybersecurity certification and cyber essentials plus respectively. Note however, that the controls are defined in an open way, leaving the CSP the room to interpret that certain of these certifications are equivalent to the standard required. The legal expert may ask the CSP exactly which certification they have and, when relevant, what certification or accreditation they consider equivalent to the examples listed in the control itself.

2.4 Short names for the controls to facilitate inclusion in the matrix

For each control, a short name is defined to add them into the matrix in a practical manner. The short names are as follows:

Table 6. Short names for the controls for inclusion in the matrix of the legal level

Control	Short name of the control in the matrix
Valid company registration	Valid company registration
Presence of a DPO/data protection point of contact	DPO/data protection point of contact
Presence of a representative in the EU (if relevant)	Representative (if relevant)
Presence of a data transfer mechanism declared by the CSP (if relevant)	Data transfer mechanism (if relevant)
Assessment of the data transfer mechanism (if relevant)	Data transfer mechanism assessment (if relevant)
Presence of data processing agreement (DPA)	Data processing agreement (DPA)
Assessment of the scope of the DPA	DPA scope
Assessment of the obligation in the DPA for the CSP to only process data on the documented instructions of the CSP's counterparty	Documented instructions only

Control	Short name of the control in the matrix
Assessment of confidentiality obligations in the DPA for persons authorized to process data on behalf of the CSP	DPA confidentiality
Assessment of the obligation in the DPA for the CSP to take all security measures pursuant to Article 32 GDPR	CSP security A32 GDPR
Assessment of the obligations in the DPA in relation to initial sub-processor engagement by the CSP	Sub-processor engagement
Assessment of the obligation in the DPA in relation to the contractual pushdown of data protection terms on a sub-processor of the CSP	Contractual pushdown sub-processor
Assessment of the obligation in the DPA stating that the CSP remains liable for a sub-processor's failures to fulfil its obligations	Sub-processor liability coverage
Assessment of the obligation contained in the DPA for the CSP to take the necessary measures to assist its counterparty with data subject requests	Data subject request assistance
Assessment of the obligation contained in the DPA for the CSP to support its counterparty with its own obligation to ensure security of processing (Article 32 GDPR)	Counterparty security measures assistance
Assessment of the obligation contained in the DPA for the CSP to support its counterparty with data breach notifications to the supervisory authority and/or the data subject	Data breach notification assistance
Assessment of the obligation contained in the DPA for the CSP to support its counterparty with data protection impact assessments (DPIAs) and, where applicable, prior consultation with the supervisory authority	DPIA assistance
Assessment of the obligation in the DPA for the CSP to delete or return (at the choice of the counterparty) all personal data at the end of the contract	Deletion or return of data
Assessment of the obligation in the DPA for the CSP to provide its counterparty with all information necessary to demonstrate compliance	Compliance information obligation
Assessment of the obligation in the DPA for the CSP to allow for and contribute to audits, including inspections, conducted by the counterparty or another auditor mandated by the counterparty	Audit rights granted
Assessment of the obligation in the DPA for the CSP to immediately inform its counterparty if, in the CSP's opinion, an instruction infringes applicable data protection law	Illegal instructions notification obligation
Assessment of liability clauses under the DPA (if relevant)	DPA liability coverage (if relevant)

Control	Short name of the control in the matrix
Assessment of termination clause under the DPA (if relevant)	Termination possibilities DPA (if relevant)
Assessment of the contractual terms on alternative dispute resolution mechanisms (if relevant)	Assessment of ADR mechanisms (if relevant)
Assessment of the contractual terms on termination of the contract with regards to the ease with which the CSP's counterparty can terminate the contract	Termination options of CSP's counterparty
Assessment of the contractual terms on termination of the contract with regards to the options available to the CSP to terminate or suspend the contract	Termination/suspension options CSP
Assessment of the contractual terms on changes to the contractual documents with regards to the level of protection offered to the CSP's counterparty from potentially disruptive unilateral changes of contract	Limitation of unilateral changes by CSP
Assessment of the general contractual terms on liability and the limitation thereof	Liability coverage
Assessment of contractual terms relating to force majeure	Force majeure coverage
Assessment of general contractual terms on confidentiality	Confidentiality terms (general)
Presence of ISO 27001 certification or equivalent covering the service	ISO 27001 or equivalent
Presence of Cloud-specific certification that meets all CCSM security objectives	Cloud certification covering all CCSM objectives
Presence of adherence to a Code of Conduct for Data Portability and Cloud Service Switching	Adherence to Data Portability and Switching Code of Conduct
Presence of adherence to a Data Protection Code of Conduct for Cloud Service Providers	Adherence to Data Protection Code of Conduct

2.5 Matrix of the legal level and explanation

As explained in section 2.1 on the concept of the legal level, one of the main struggles is to give weight and importance to the controls defined under section 2.2. While this may in part depend on the specific requirements of the target user organization, a functioning general legal level in ACSmI must be able to do this in a general and abstract manner.

It must be defined what controls are basic and relevant for every organization and must thus minimally be present for a Cloud service to attain the legal level tier 3, i.e. the minimal legal level. Equally, it must be decided which controls are more advanced and not necessarily relevant for every organization. These are the necessary building blocks for the legal level as a composite of controls, which must be differentiated between in order to create tiers in the legal situation offered by the CSPs for the different Cloud services in ACSmI.

For the simple controls, since no differentiation is possible within the control itself, additional differentiation will be necessary to insert these controls into the legal level. Therefore, to build the legal level, the simple controls will be marked as one of the following:

- Must have

- Should have
- Nice to have

This determination will translate into inclusion of the legal level as follows:

- Tier 3 will contain at least all the “must haves”
- Tier 2 will contain all the “must haves” and the “should haves”
- Tier 1 will contain all the “must haves”, all the “should haves” and the “nice to haves”

Note that controls marked as “if relevant” are only taken into account when they are relevant. If they are not, then the control is not taking into account when determining the legal level.

The simple controls are classified as follows:

Table 7. Assigning importance to simple controls

Control	Must have	Should have	Nice to have	Justification
Valid company registration	X			The CSP must be valid company in order to be able to act against it, should that be necessary. This is a most basic requirement for any business partner in general, and thus must be marked as a “must have”.
DPO/data protection point of contact	X			Having a DPO or privacy officer appointed is a basic commitment to data protection on the CSP’s part. Absence of a DPO or privacy officer would be a good reason to not engage the CSP, hence the qualification as a must have.
Representative (if relevant)	X			If relevant, this is another basic commitment to compliance with the GDPR. Absence of a representative when required by law would be a good reason to not engage the CSP, hence the qualification as a must have.
Data transfer mechanism (if relevant)	X			If relevant, a data transfer mechanism must be present. Without such a mechanism any transfer is illegal and a compliance risk. Absence of a data transfer mechanism would be a good reason to not engage the CSP, hence the qualification as a must have.
Data processing agreement (DPA)	X			The GDPR requires this. Absence of a DPA would be an enormous

Control	Must have	Should have	Nice to have	Justification
				oversight and compliance risk for the controller.
ISO 27001 or equivalent		X		While having certification under ISO27001 or equivalent is not a strict legal obligation and it could very well be true that a non-certified CSP does still uphold state of the art practices, this is a basic certification to have and is therefore recommended to have. Since the absence of certification does not necessarily indicate that the CSP does not maintain state of the art practices (the cost might be a prohibitive factor), it is not qualified as a must have, but rather as a should have.
Cloud certification covering all CCSM objectives			X	A Cloud-specific certification covering all CCSM objectives shows an advanced commitment of the CSP to maintaining and proving a high level of security. This is neither necessary (so not a must have) nor should it be recommended to all Cloud users (so not a should have). However, for those having high compliance needs or with a very small risk appetite, this can be an additional guarantee. Hence the designation as “nice to have” in general terms.
Adherence to Data Portability and Switching Code of Conduct			X	This control is based on Code of Conducts which is still in an early stage. To make this anything else than a “nice to have” would be to unreasonably impose upon CSPs the requirement to be an early adopter. This control may be given a different weight in the future, as the uptake of Codes of Conduct becomes more standard.

Control	Must have	Should have	Nice to have	Justification
Adherence to Data Protection Code of Conduct			X	This control is based on Code of Conducts which is still in an early stage. To make this anything else than a "nice to have" would be to unreasonably impose upon CSPs the requirement to be an early adopter. This control may be given a different weight in the future, as the uptake of Codes of Conduct becomes more standard.

For the layered controls, differentiation is already present within the control itself. The legal expert will assign the Cloud service with zero to three stars on every layered control. Zero stars should always lead to an exclusion of the service, i.e. this will prevent the service from being onboarded in ACSmI.

Services that score at least one star on every layered control are allowed into ACSmI and are therefore awarded a legal level. It follows from this that a Service of legal level tier 3 has:

- All "must have" simple controls ticked; and
- At least one star for all layered controls

Now, the more important step is to define what differentiates a legal level tier 3 (the baseline) from tier 2 (medium protection) and tier 1 (high protection). For the simple controls this is defined in the table above. For the layered controls, the question is more complex.

One option would be to require all layered controls to have two stars for tier 2 and 3 stars for tier 1 since the differentiation is already present in the control itself, as mentioned above. There are however good reasons not to do this:

- This simplified approach would ignore the important fact that not all controls are equally important; and
- This would mean that as soon as a CSP would score one star below the stars needed for a certain tier, even on a control of relative minor importance, it would fall back a whole tier; and
- For the same reason, it would be doubtful if any CSP would be able to attain tier 1. Many CSPs might even struggle to attain tier 2 if they would score one star on a control of relative minor importance (e.g. the quality of the ADR clause, which is often debatable).

For this reason, the layered controls must be further differentiated too. The following table defines how many stars are respectively needed for each control to constitute tier 2 and tier 1 and the justification for this.

The reasoning is as follows:

- Important controls should have two stars (medium level of protection) in tier 2 and three stars (high level of protection) in tier 3;
- Controls of lesser importance can have less than two (medium level of protection) or three stars (high level of protection) in tier 2 and 3 respectively.

Table 8. Assigning importance to layered controls

Control	Stars required for legal level tier 2	Stars required for legal level tier 1	Justification
Assessment of ADR mechanisms (if relevant)	1	2	ADR clauses are often inadequately described. Moreover, the absence of enforceable ADR options does not necessarily present a lower level of protection. Hence, while it is a relevant factor to have enforceable ADR options, that are preferably not binding on the CSP's counterparty (e.g. an expensive arbitration), this control is comparatively of lesser importance in the multi-Cloud context of DECIDE. Moreover, in many situations services might be procured through ACSmI, so the DECIDE user may not be the entity involved in any litigation at all.
Termination options client	1	2	While this is not unimportant, the continuity of the service is not affected here. As with the above control, in many situations, it might be so that ACSmI will have a direct contract with the CSP and will re-sell the services, so this will not likely be the most relevant requirement for the DECIDE user. Hence the qualification as a control of lesser importance.
Liability coverage	1	2	This control concerns the general liability coverage. This is generally not the biggest concern in Cloud, as liability is typically strongly capped and damages may be hard to pursue. Additionally, as with the previous controls, there might be many instances in which the contract with the CSP will be with ACSmI directly. In that case the liability coverage is of even lesser importance to the DECIDE user. Hence the qualification as a control of lesser importance.
Force majeure coverage	1	2	This control concerns the other side of the coin of liability coverage. To the extent that force majeure applies, the CSP will in any case not be liable. This is generally not the biggest concern in Cloud, as liability is typically strongly capped and damages may be hard to pursue. Additionally, as with the previous controls, there might be many instances in which the contract with the CSP will be with ACSmI directly. In that case the liability coverage is of even lesser importance

Control	Stars required for legal level tier 2	Stars required for legal level tier 1	Justification
			to the DECIDE user. Hence the qualification as a control of lesser importance.
Data transfer mechanism assessment (if relevant)	2	3	This is an important control since the absence of an adequate mechanism leads to the illegality of the transfer.
DPA scope	2	3	This is an important control, given that a clear DPA scope is a strict GDPR requirement incumbent on the controller. Hence this is relevant for the DECIDE user, or its clients/intended customers, to ensure their GDPR compliance.
Documented instructions only	2	3	This is in important control given that this is a strict GDPR requirement incumbent on the controller. Hence this is relevant for the DECIDE user, or its clients/intended customers, to ensure their GDPR compliance. Moreover, it also ensures that the controller has a measure of control over the processing.
DPA confidentiality	2	3	This is an important control. Next to be a strict GDPR requirement like the previous controls, it also ensures the confidentiality of any personal data that might be contained in the micro-service(s) of the multi-Cloud application deployed with the CSP.
CSP security A32 GDPR	2	3	This is an important control. Next to be a strict GDPR requirement like the previous controls, it ensures that the CSP has undertaken a sufficiently clear obligation to implement appropriate security measures, not only for today but also for the future.
Sub-processor engagement	2	3	This is an important control. Next to be a strict GDPR requirement like the previous controls, clear and enforceable rules on sub-processor engagement are necessary because in many cases the application developer as a DECIDE user will end up becoming a processor itself of its potential clients for the application. Hence, as a first processor, it is important for them to keep track of the chain of processing. The contractual obligation binding the CSP enables a measure of control.
Contractual pushdown sub-processor	2	3	This is an important control. Next to be a strict GDPR requirement like the previous controls, clear and enforceable rules on contractual pushdown of the same data

Control	Stars required for legal level tier 2	Stars required for legal level tier 1	Justification
			protection terms on any sub-processors of the CSP are necessary because in many cases the application developer as a DECIDE user will end up becoming a processor itself of its potential clients for the application. Hence, as a first processor, it is important for them to keep track of the chain of processing and to ensure that standards of data protection are respected throughout. The contractual obligation binding the CSP to push down contractual terms enables a measure of control.
Sub-processor liability coverage	2	3	This is an important control. Next to be a strict GDPR requirement like the previous controls, clear and enforceable rules on liability for the sub-processors of the processor engaging them are necessary because in many cases the application developer as a DECIDE user will end up becoming a processor itself of its potential clients for the application. Hence, as a first processor, they will bear against their clients-controllers the full liability for any sub-processor failure, including the CSP (!). Therefore, it is important for them to keep track of the chain of processing and to ensure that the CSP is contractually bound to carry responsibility for its sub-processors. The contractual obligation binding the CSP to cover the liability of their own sub-processors enables a measure of control.
Data subject request assistance	2	3	This is an important control. Next to the GDPR strictly requiring such a clause, assistance of the CSP may be needed at times to be able to fulfil data subject requests. Such assistance needs to be contractually secured by the application developer, whether controller or processor (in that case for its clients).
Counterparty security measures assistance	2	3	This is an important control. Next to the GDPR strictly requiring such a clause, it may be needed for the CSP to lend assistance in efficiently obtaining and organizing a high level of security for the application. This is relevant both when the application

Control	Stars required for legal level tier 2	Stars required for legal level tier 1	Justification
			developer is the controller as when the application developer is a processor.
Data breach notification assistance	2	3	This is an important control. Next to the GDPR strictly requiring such a clause, it is of utmost importance for a data breach to be communicated and notified asap and at least within the legal time limits. Clear obligations help achieve this, both when the application developer is the controller as when it is a processor.
DPIA assistance	2	3	This is an important control. Next to the GDPR strictly requiring such a clause, the CSP's input might sometimes be needed in order to identify all necessary elements for a DPIA (e.g. details on the security measures in place). Clear obligations help achieve this, both when the application developer is the controller as when it is a processor.
Deletion or return of data	2	3	This is an important control. Not only does the GDPR require an obligation on this, it also ensures that the data does not stay with the CSP. This is relevant whether the application developer is a controller or a processor.
Compliance information obligation	2	3	This is an important control. Not only does the GDPR require an obligation on this, obtaining sufficient compliance information enables the controller (the application developer or its client) to assess the CSPs compliance situation. A broad obligation for the CSP to make this available helps things along nicely.
Audit rights granted	2	3	This is an important control. Not only does the GDPR require an obligation on this, this is the essential measure to really verify whether a CSP lives up to its promises, which is especially useful and necessary when there are reasons to doubt the CSPs contractual claims. An important obligation therefore, whether or not the application developer is controller or processor.
Illegal instructions notification obligation	2	3	This is an important control. Not only does the GDPR require having language on this, it is an important mechanism to leverage the CSPs expertise to the benefit of its counterparty (and their clients).

Control	Stars required for legal level tier 2	Stars required for legal level tier 1	Justification
DPA liability coverage (if relevant)	2	3	This is an important control. If the DPA contains a provision on this, this may severely increase risk if the CSP tries to get out of liability for GDPR matters. This liability may be quite relevant since fines can be very high under the GDPR.
Termination possibilities DPA (if relevant)	2	3	This is an important control. If the CSP should be able to terminate the DPA before the provision of services is terminated as well, essentially a situation of non-compliance with Article 28 GDPR would be created. Therefore, this must, if such language is present in the contract, be assessed as equally important to any Article 28 GDPR requirement.
Termination/suspension options CSP	2	3	In the multi-Cloud context, although it presupposes a dynamic use of Cloud resources, it is nonetheless relevant that there is some continuity of service guaranteed by the CSP to its customer. Hence, termination or suspension options available to the CSP are an important control as it might impact the functioning of the whole application.
Limitation of unilateral changes by CSP	2	3	In the multi-Cloud context, although it presupposes a dynamic use of Cloud resources, it is nonetheless relevant that there is some continuity of service guaranteed by the CSP to its customer. Hence, the extent to which a CSP can unilaterally make changes to the contract is relevant to assess to what extent the CSP could unilaterally cause a given service to no longer fit the application's needs, which may put the application developer in a tough spot if no other services offer the same result. Hence, this is an important requirement.
Confidentiality terms (general)	2	3	Contrary to the other general contract requirements, confidentiality may be a more sensitive topic and thus must be classified as important. Confidentiality under the DPA after all only covers processing of personal data and thus does not cover non-personal data processing by the CSP. Nonetheless, confidentiality may be very important here as well, as this information may relate to

Control	Stars required for legal level tier 2	Stars required for legal level tier 1	Justification
			corporate and trade secrets, IP protected matters and other confidential information, whatever its nature. For this reason, a clear and enforceable confidentiality obligation in the contract is an important safety net.

Note that controls marked as "if relevant" are only taken into account when they are relevant. If they are not, then the control is not taken into account when determining the legal level.

The Cloud service is awarded the legal level of which it meets all the requirements.

The following table contains the final legal matrix, based on the aforementioned rules and results. Note that controls have been re-arranged slightly to make the matrix clearer.

Table 9. Legal level matrix

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
Simple controls			
Valid company registration	✓	✓	✓
DPO/data protection point of contact	✓	✓	✓
Representative (if relevant)	✓	✓	✓
Data transfer mechanism (if relevant)	✓	✓	✓
Data processing agreement (DPA)	✓	✓	✓
ISO 27001 or equivalent	✗	✓	✓
Cloud certification covering all CCSM objectives	✗	✗	✓
Adherence to Data Portability and Switching Code of Conduct	✗	✗	✓
Adherence to Data Protection Code of Conduct	✗	✗	✓
Layered controls			

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
Assessment of ADR mechanisms (if relevant)	★	★	★★
Termination options of CSP's counterparty	★	★	★★
Liability coverage	★	★	★★
Force majeure coverage	★	★	★★
Data transfer mechanism assessment (if relevant)	★	★★	★★★
DPA scope	★	★★	★★★
Documented instructions only	★	★★	★★★
DPA confidentiality	★	★★	★★★
CSP security A32 GDPR	★	★★	★★★
Sub-processor engagement	★	★★	★★★
Contractual pushdown sub-processor	★	★★	★★★
Sub-processor liability coverage	★	★★	★★★
Data subject request assistance	★	★★	★★★
Counterparty security measures assistance	★	★★	★★★
Data breach notification assistance	★	★★	★★★
DPIA assistance	★	★★	★★★
Deletion or return of data	★	★★	★★★

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
Compliance information obligation	★	★★	★★★
Audit rights granted	★	★★	★★★
Illegal instructions notification obligation	★	★★	★★★
DPA liability coverage (if relevant)	★	★★	★★★
Termination possibilities DPA (if relevant)	★	★★	★★★
Termination/suspension options CSP	★	★★	★★★
Limitation of unilateral changes by CSP	★	★★	★★★
Confidentiality terms (general)	★	★★	★★★

2.6 Assigning and monitoring the legal level

2.6.1 Procedure

This section aims to clarify the flow of assigning and monitoring the legal level in ACSmI.

Assigning the legal level happens during the onboarding process of a Cloud Service in ACSmI.

The following procedure assumes that the CSP is actively engaged in the process. Please note however, that technically, this can also be done without the CSP engaged, through personnel of the entity exploiting ACSmI acting in the CSP role. This is however not preferable because of the legal risks and the lack of enforceable terms against the CSP set out in section 3.

The **process of assigning the legal level** is as follows:

- Step 1: the CSP enters into a contract with the entity exploiting ACSmI, including the assurance policy on the legal level and accepting that its answers on the questions in step 2 are binding, as well as the contractual documents they choose to provide at that time (see on this section 3 “A contractual framework for the legal level;

- Step 2: the CSP uploads its contractual documents and answers the questions based on the simple controls. These answers and the contractual documents are made available to the legal expert.

- Step 3: the legal expert reviews the answers of the CSP and the contractual documents. The legal expert answers all the questions related to the layered controls and provides a short explanation per question.

- Step 4: the legal expert determines the legal level based on the results of step 3 and as explained in this document. The Cloud service is assigned the highest legal level for which it meets all requirements as set out in the matrix.

- Step 5: The Cloud service is assigned the legal level in ACSmI and this is communicated to the CSP.

- Step 6: if the CSP is unhappy with the legal level assigned, it can request the reasoning of the legal expert.

- Step 7: With the explanation in hand, the CSP can adapt its contracts or provide additional information to the legal expert. A dialogue may be started.

- Step 8: the legal expert will react to these changes by providing an updated assessment, the result of which may vary from the initial assessment.

- Step 9: if the CSP remains unhappy, it can withdraw its service from ACSmI within a given time limit.

- Step 10: the legal level is finalized, and the service can be utilized in ACSmI.

After onboarding a service into ACSmI and assigning the legal level, a second process starts, namely the **process of continuous monitoring of the legal level.**

Specifically, there are four events which will trigger a reassessment of the legal level and must be monitored:

- A CSP changes its contracts, which it will have to report to the entity exploiting ACSmI under the contract with the CSP. The assurance policy will detail what changes are substantial enough to trigger this process.

- A CSP makes changes which affect its answers to the questions based on the simple controls, which it will have to report to the entity exploiting ACSmI under the contract with the CSP. The assurance policy will detail what changes are substantial enough to trigger this process.

- There is an important change in legislation, case law or interpretation, which requires reassessing all or certain contracts. This is monitored by the legal expert. The assurance policy will detail which changes will trigger this process.

- Changes other than in the CSP's legally relevant situation in specific or in legislation, case law or interpretation which nonetheless has a measurable impact on the controls of the legal level. Events that might qualify are substantive changes in standards, market standards, market expectations, state of the art, etc. If such external factors warrant a re-assessment of the legal level by adding, deleting or changing controls, or by impacting the interpretation to be given to certain controls, this may lead to a re-assessment of the legal level assigned to a given service. Such changes will be identified by the entity exploiting ACSmI and will be implemented with prior notice only and to all CSPs indiscriminatorily. The assurance policy will detail this process.

In either of these eventualities, steps 3 and further above are repeated, taking into account the new information.

2.6.2 Guidance to the legal expert and consistency

Given that the legal expert will to some extent enjoy a margin of appreciation when assigning the legal level, it is important to provide enough guidance and ensure consistency of the approach taken.

First, to provide proper guidance, the basis will be this white paper. The controls as defined in section 2.2 and subsections above already provide guidance on how to answer the questions the legal expert has to answer. In addition, however, there will be an updated repository of legislation, case law and other official documents available to the legal expert or experts. Moreover, a log will be kept of prior assessments, to provide guidance in tough cases, as well as to ensure consistency.

Consistency across assigning the legal level needs to be ensuring on two levels. First, the legal expert must treat all CSPs equally, i.e., there must not be a different result based on nearly identical contracts. Second, there must be a mechanism for consistency if the role of the legal expert should be fulfilled by several natural persons.

To address consistency across reviews in general, a log will be kept that can at any time be consulted by the legal expert to compare contractual language with previous assessments and results of potentially comparable language. This log will contain the legal expert's motivation in that case as well. This log could moreover be made accessible to the CSP to ensure transparency. In any case the CSP will receive the motivation of the legal expert in its own case and will have access to the whitepaper and other information under the assurance policy, enabling it to verify whether the legal expert's review has been consistent with the principles set out in this whitepaper.

To address consistency in the case several natural people are working as legal experts at any time, there will be a head legal expert who will review all cases before assigning a legal level, as well as the existing log, so as to maximally ensure consistency in assigning the legal level at any given time.

2.7 The legal level as a non-functional requirement in ACSmI

As explained already in D5.3 and illustrated in the foregoing, the legal level will function as an additional non-functional requirement (NFR) of the multi-Cloud application, (in a way) just like cost or availability.

NFRs are stored in the application description and can be altered. Thus, the legal level can be altered during the lifetime of the application to show the ever-evolving understanding of the legal needs of the target user organization(s).

NFRs have the effect of pre-selecting or pre-rejecting certain Cloud services, since OPTIMUS will only elicit those services from ACSmI to propose them and use them for deployment that meet all the NFRs of the application. The legal level therefore has this effect as well.

Thus, when an application developer enters tier 2 as an NFR in the application's description, only Cloud services that have been assigned legal level tier 2 (or higher) in ACSmI will be proposed and used for deployment.

It is important to be reminded as a fact that the legal level is a minimal requirement. The requirement may always be outperformed by the CSP. Thus, a Cloud service with tier 2 which is more expensive than the tier 1 one should not prevail because the application description requires tier 2. What it really requires is tier 2 or higher.

At this point it is important to see the interplay between different NFRs as well. Say cost and availability are the two other NFRs. Then OPTIMUS will request information from ACSmI and propose the Cloud services which:

- At least meets the required legal level; and
- At least meets the required availability; and
- Are the most affordable

2.8 Proof of concept of assigning the legal level

In this section the legal level will be assigned to two example Cloud Services, as a proof of concept. They represent steps 3 and 4 described in section 2.7 above.

Example 1 is a Cloud service offered by a SME CSP. Since the CSP is based in the EU offers services in the EU and abroad. The service chose is carried out completely and solely in the EU.

Example 2 is a Cloud service offered by a large CSP (such as Amazon, Microsoft Azure or Google Cloud). The CSP is based in the US, but offers services in the EU too, without data transfers. The service chosen is carried out completely and solely in the EU.

The proof of concept is meant to show how the legal level would be assigned, but with the caveat that for the simple controls some assumptions will have to be made as to the answers of the CSP.

Of course, this will be programmed into ACSmI so the layout might change. For reasons of clarity, the control above are repeated and the answer selected by the legal expert is highlighted in green, follow by a justification of this answer, which could then be reviewed by the C SP if requested (see on this section 2.7 above).

The contracts used are those currently in force at the CSP, respectively provided directly by the consortium partner and found on the CSP's website online.

The proof of concept is done anonymously to avoid bias of any sort.

2.8.1 Example 1: selected SME CSP Cloud service

Simple controls

Question to the CSP	Answer
Is your organization a validly registered and incorporated entity, which is neither in liquidation nor in a state of bankruptcy?	Yes
Did your organization appoint and will it maintain a DPO in accordance with Articles 37-39 of the GDPR or an equivalent position e.g. a privacy officer or privacy team which can act as a data protection point of contact?	Yes
Do you provide a data processing agreement which is compliant with Article 28 of the GPDR?	Yes
Did your organization obtain and does it maintain a certification under the ISO 27001 standard or equivalent, covering the service in question?	Yes
Did your organization obtain and does it maintain at least one certification that meets all of the 27 security objectives of the Cloud Certification Schemes Metaframework as defined by ENISA, such as CSA attestation/certification – OCF level 2, TÜV Rheinland Certified Cloud Service certification or equivalent and which covers the service in question?	No
Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting reasonable industry standards for data portability	No

and switching as intended by Article 6 of the Regulation on the free flow of data?	
Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting out data protection requirements, approved under Article 40 GDPR?	No

Layered controls

Control	**Adequacy of the scope description in the DPA, as required by Article 28(3) GDPR.**
Question (for the legal expert)	How would you assess the description of subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects as required by Article 28(3) GDPR in the DPA under revision?
Possible answers	Description not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clause is present with clear description.
Control	**Adequacy of the contractual obligation for the CSP as a (sub-) processor to process personal data, including with regards to data transfers outside the EEA, only on the documented instructions of the CSP's counterparty, as prescribed by Article 28(3), a) GDPR, unless required to do so by EU or member state law, in which case the CSP has to inform its counterparty of that legal requirement, unless that in itself is forbidden by the legal rule in question.**
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP as a (sub-)processor to only act on the documented instructions of the CSP's counterparty, in the light of Article 28(3), a) of the GDPR and the current official interpretation available?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).

	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clauses in contract fail to state explicitly that only on the documented instructions data will be processed, although this is the meaning to be gathered from the different clauses that mention this topic.
Control	**Adequacy of the contractual obligation for the CSP to ensure confidentiality of personnel and agents authorized to process data on its behalf through commitments of confidentiality or by the relevant persons being under a statutory obligation of confidentiality, as prescribed by Article 28(3), b) GDPR.**
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP to ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clause is present, clear and even more extensive than required by law.
Control	**Adequacy of the contractual obligation for the CSP to take the appropriate technical and organizational measures to ensure a level of security appropriate to the risk, pursuant to Article 32 GDPR, as prescribed by Article 28(3), c) GDPR.**
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP to take all security measures pursuant to Article 32 GDPR, in the light of the obligation of Article 28(3), c) GDPR to include a clause detailing such measures in the DPA?
Possible answers	Obligation not present.
	Present, but potentially faulty (e.g. making the controller agree that a certain set of current measures will forever be appropriate) or unclear

	description given the context of the given CSP (reservation), so that it may be insufficient under Article 28(3), c) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), c) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	The obligation is open-ended and general, so the CSP's counterparty is not bound to accept a given set of measures as sufficient, which would be negative. However, the contractual documents do give examples of measures taken and list the measures currently taken with some detail. This is the best of both worlds.
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the engagement of sub-processors by the CSP, specifically the need to have prior general or specific written authorization, and, in the case of general authorization, to inform its counterparty of intended changes, offering its counterparty an opportunity to object to such changes, as prescribed by Article 28(3), d) and 28(2) GDPR.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(2) GDPR, as referred to in Article 28(3), d) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonably short delays, an infeasible manner of objection, or other conditions arguably hollowing out the legally intended effect of Article 28(2) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	There is prior notification of changes, but notification period is not specified. CSP's counterparty can object within a reasonable although not very extensive period and can terminate the agreement or purchase related to that sub-processor if the objection is not unreasonable. These are fair commercial terms that do not seem to hollow out the intended effect of Article 28(2) GDPR. However,
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the consequences of engaging a sub-processor, namely that the same data protection obligations binding the CSP to the**

	CSP's counterparty should be passed down to the sub-processor of the CSP, as prescribed by Article 28(3), d) GDPR and Article 28(4) GDPR.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with the requirement of pushing down the same data protection terms binding the CSP on any sub-processors engaged in the processing by the CSP, as described in Article 28(4) GDPR, as referred to in Article 28(3), d) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential limitations or obscurity created by the contract terms which may be interpreted as such, arguably hollowing out the legally intended effect of Article 28(4) GDPR. (Low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	The contract specifies they will push down the exact same terms.
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the consequences of engaging a sub-processor, namely that there should be a clear affirmation that the CSP shall in any case remain liable towards the CSP's counterparty for failure of its sub-processor to perform its obligations, as prescribed by Article 28(3), d) GDPR and Article 28(4) GDPR.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(4) GDPR, as referred to in Article 28(3), d) GDPR, namely that there should be a clear statement that the CSP will always remain liable towards its counterparty if the CSPs sub-processor fails to fulfil its obligations?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential limitations or obscurity created by the contract terms which may be interpreted as such, arguably hollowing out the legally intended effect of Article 28(4) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).

	Present and fully adequate (high protection).
Justification of answer	Contract specifies that any shortcoming of a sub-processor shall be treated as if committed by the CSP itself.
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the CSP assisting its counterparty, by appropriate technical and operational measures insofar as this is possible, to respond to data subject requests, as prescribed by Article 28(3), e) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including those relating to cost and conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(3), e) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of high costs, unreasonable conditions or other, arguably hollowing out the legally intended effect of Article 28(3), e) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), e) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Obligation is present a clearly described, although with some small caveats in the language. In addition, there is a clear clause on what happens if the CSP is contacted directly by data subjects and in this case the CSP will provide support provided that the counterparty will cooperate where necessary and reimburse the costs.
Control	**This control relates to the adequacy of the contractual obligation in the DPA with regards to the CSP's obligation to assist its counterparty in attaining an adequate level of security of processing as meant in Article 32 GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including those relating to cost and conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide assistance to its counterparty in the counterparty's own obligation to ensure an adequate level of security of processing, as required by Article 28(3), f) GDPR?

Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of high costs, unreasonable conditions or other, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Present but minimal language, hence the designation as medium protection.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to support its counterparty with the latter's obligation to notify the supervisory authority and/or the data subject in case of a data breach, likely to result in a (high) risk for data subjects, as provided in Article 28(3), f) GDPR, 33 GDPR and 34 GDPR. It assesses the content of that obligation in the DPA and its potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide support in fulfilling the notification obligations of Article 33 and 34 GDPR as required by Article 28(3), f) GDPR, specifically outside the own processor-specific obligation to notify the controller without undue delay after becoming aware of a data breach (Article 33(2) GDPR)?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clear obligation, fully adequate assistance description, without any need for remuneration.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to support its counterparty with the latter's obligation**

	to carry out a data protection impact assessment (DPIA) on intended processing activities that meet the requirements set by Article 35 GDPR (likely to result in a high risk for the data subject) and to consult with a supervisory authority prior to carrying out the planned processing activity when the outcome of the data protection impact assessment is that there is a high residual risk, despite the risk containment and prevention measures already taken by the counterparty and detailed in the DPIA, i.e. that there is a high risk remaining in the absence of further controlling measures to be taken by the controller (Article 36 GDPR). It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide support in fulfilling its counterparty's obligation to carry out a data protection impact assessment under the conditions provide in Article 35 GDPR and, where applicable, of the prior consultation obligation contained in Article 36 GDPR, as required by Article 28(3), f) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, unreasonably high costs, lack of capacity of the counterparty to decide when a data protection impact assessment or prior consultation is necessary, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Present but minimal language, hence the designation as medium protection.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to delete or return, at the choice of its counterparty, all personal data of the controller at the end of the contract, unless EU or member state law specifically requires further storage of that data, as defined in Article 28(3), g) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to, a choice

	of the counterparty, delete or return all personal data to the counterparty at the end of the provision of services?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), g) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), g) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Reasonable period of delay, certificates are offered to prove deletion. Some caveat for longer retention services but deletion can always be requested prior to this term. Options exist to retrieve the data as well if the counterparty should prefer this.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to provide its counterparty with all compliance information necessary, specifically to show the CSP's compliance with the obligations defined by Article 28, as defined in Article 28(3), h) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP to make available to its counterparty all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), h) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), h) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Present and clear, but subject to a fee. Hence medium protection.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to allow for and contribute to audits, including inspections either carried out by the counterparty itself or by another**

	auditor mandated by the counterparty, as required explicitly by Article 28(3), h) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP submit itself to audits, including inspections carried out by the counterparty itself or by another auditor mandated by the counterparty, as required by Article 28(3), h) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions (high costs, long delays, etc.), carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), h) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), h) GDPR (medium protection).
	Present and fully adequate, providing for real audit and inspection rights at reasonable conditions for the counterparty (high protection).
Justification of answer	Obligation present and clear. Audits are proposed in a limited manner consisting of document and reports review prepared by the CSPs auditor, although the CSP's counterparty may require at will a more extensive audit. Such an audit shall however be fully financed by the counterparty and its scope must be agreed beforehand, next to some standard other conditions. Thus, there is a real audit possibility, but the level of protection is medium since a) the counterparty has to bear all the costs and b) the CSP has to agree on the scope, so this could be a pitfall too.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to immediately inform the counterparty if any of its instructions are, in the opinion of the CSP, contrary to applicable data protection law (GDPR, EU law or member state law).**
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP to immediately inform the counterparty if it considers any of the counterparty's instructions contrary to applicable data protection law as required by Article 28(3), second subparagraph GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential delays, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), second subparagraph GDPR (low protection).

	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), second subparagraph GDPR (medium protection).
	Present and fully adequate (high protection).
Justification	Clear obligation, adequate and enforceable.
Control (if relevant)	**This control aims to assess the liability clause in the DPA, if any are present, even by reference to other contractual documents. Liability clauses in the DPA specifically may be different from the general liability clause, and have to be in accordance with Article 82 GDPR.** **The control looks at all liability clauses for data protection matters, including liability towards data subjects, liability for fines and related matters of liability. The full liability for sub-processors that the CSP has to guarantee under Article 28 can also be relevant here, since that Article requires "full liability". Thus a statement in the previous control of full liability could be curtailed by a limiting liability clause.** **Note: If no clause is present, this control is not considered, since it cannot in general terms be stated whether or not this is a positive or a negative point.**
Question (for the legal expert)	How do you assess the liability situation for data protection related matters (liability towards data subjects, for fines, for related matters, full liability of the processor for the sub-processor) under the DPA, especially in the light of Article 82 GDPR and taking into account the impact of that Article on the principal freedom of contract of the Parties?
Possible answers	Exclusions are present in a wording clearly in direct conflict of the GDPR, e.g. conflicting with the terms of Article 82 GDPR or providing for backdoor circumvention of Article 28(4) GDPR.
	The DPA contains some clear liability caps, limitations and/or exclusions, the text of which may be in conflict with the GDPR and/or are very negative for the counterparty (reservation) (low protection).
	The DPA contains liability caps, limitations and/or exclusions, the text of which is likely compliant with the GDPR and provides at least a reasonable measure of balance between the contracting parties (medium protection)
	The DPA contains liability caps, limitations and/or exclusions which are balanced and clearly within the margin of appreciation of the parties, not depriving the contract of its essence (high protection).
Justification of answer	There is only a liability cap for matters between the CSP and the counterparty. The liability cap is arguably reasonable and does not seem to deprive the contact of its essence.

Control (if relevant)	**This control addresses the termination clause of the DPA, if there is any. Such a clause is not obligatory but if present must not limit the effect of the DPA. In practice such clauses are nonetheless found and they have the effect of hollowing out the intended effect of article 28 GDPR. This control aims to assess this potential threat.** **Note: If no clause is present, this control is not considered, since it cannot in general terms be stated whether or not this is a positive or a negative point.**
Question (for the legal expert)	If there is a termination clause in the DPA, does it ensure protection of the CSP's counterparty and compliance under article 28 GDPR?
Possible answers	No, the DPA can easily be terminated, leaving the service contract of the services that contain the processing activities intact, without a valid DPA.
	This is unclear, the wording of the contract is vague or faulty, or there is a reference which does not contain specific language on this topic; it could reasonably be questioned whether this clause has the effect of hollowing out Article 28 GDPR (reservation) low protection.
	The DPA's termination clause is reasonably formulated and to be interpreted as logically following the main service agreement; it is unlikely to be interpreted as hollowing out Article 28 GDPR (medium protection).
	The DPA's termination clause is clearly worded and leaves no or little room for misinterpretation. The DPA logically follows the main contract. It is very likely compliant with the GDPR and does not hollow out Article 28 GDPR (high protection).
Justification of answer	Clear clause, no discussion possible.
Control	**This control assesses the level of the contractual possibilities to terminate the contract with the CSP. It aims to measure how flexibly the counterparty of the CSP can get out of the contract. Some termination possibilities are standard, e.g. for material breach. Others are not. Some CSPs offer very flexibly terminated contracts, while others strictly limit this, through a variety of clauses, including through the manner in which notification can be given. The consequences of termination are also taking into account.**
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms, how do you assess the level of ease offered to the CSP's counterparty in terminating the contract in a situation where the CSP's services are no longer wanted, also taking account of any consequences of termination?

Possible answers	There are unreasonable punitive clauses, limitations and exceptions or otherwise clauses which make termination very difficult.
	Termination is possible, but only in limited circumstances e.g. breach of contract, or with a very early prior notice, or under conditions which are substantially aimed to protect the CSP (reservation) (low protection)
	Termination is possible in most or all circumstances, notice periods are reasonable if any and the conditions are reasonably balanced, termination is also possible without notice under breach of contract, although grace periods may apply. (medium protection)
	Termination is very easy and always possible. No notice period applies or it is very limited. Breach of contract justifies immediate termination with little grace periods, if any. All conditions are favourable to the CSP's counterparty (high protection).
Justification of answer	Termination is always possible given 30 days written notice. Termination without notice is possible in limited circumstances given materially failure on part of the CSP, with some grace periods applying to this kind of termination too. Consequences of termination are quite standard, and therefore are not dissuasive for the use of the termination option.
Control	**This control assesses the options available to the CSP to terminate or suspend the contract and the resulting level of protection of the CSP's counterparty in continuity of the enlisted services.**
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms, how do you assess the level of protection offered to the CSP's counterparty when looking at the options available to the CSP to terminate or suspend the contract.
Possible answers	There is no protection. The CSP can terminate and/or suspend at will, with no reason or notice and there are no mechanisms to ease the transition.
	Termination and/or suspension is very easy for the CSP, many options being available with a low threshold, including options for termination/suspension without notice based on very low-threshold contractual shortcomings of the counterparty (reservation) (low protection)
	Termination and/or suspension are possible in several circumstances, but there are notice periods and/or other mechanisms to ease transition and this is reasonable. Termination/suspension without notice is only possible on the basis of reasonable conditions (medium protection).
	Termination and/or suspension are possible in a reasonably limited number of circumstances. Notice periods and/or other mechanisms to ease transition are favourable to the CSP's counterparty.

	Termination/suspension without notice is strictly limited (high protection).
Justification of answer	Notice period for the CSP is also 30 days. There are limited circumstances, clearly described, in which the CSP can terminate and suspend without notice. A few of these are not very high-threshold, however nor are they unreasonable commercially speaking. Hence the designation as medium protection.
Control	**This control assesses whether or not, and to what extent the CSP is reserving the right to unilaterally change the contractual documents. This is a provision often found in CSP contracts and may be an issues if the changed terms are unacceptable for the user. The way in which this is done and the period of notice are relevant factors to take into account. The control is measuring the level of protection for the CSP's counterparty, and thus more flexibility for the CSP means less protection in terms of guaranteed continuity for the CSP's counterparty. The absence of such a clause, which implies that the contract is permanent and more durable, is a positive point. In a way, this is the other side of the coin of the control on ease of termination for the CSP's counterparty.**
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms how do you assess the level of protection offered to the CSP's counterparty from potentially disruptive unilateral changes of contract?
Possible answers	Unilateral changes are possible, without the CSP having to give a reason, and with very little to no notice period, giving the CSP's counterparty little to no time to find alternatives if the new terms are unsuitable.
	Unilateral changes are possible, without the CSP having to give a reason, and with a short notice period, giving the CSP's counterparty some opportunity to find alternative solutions if the new terms of the contract are unsuitable (reservation) (low protection).
	Unilateral changes are possible, with or without the CSP having to give a reason, but there is a reasonable notice period and potentially other mechanisms giving the CSP's counterparty a fair opportunity to find alternative solutions if the new terms of the contract are unsuitable (medium protection).
	Unilateral changes are not possible. The contract is fixed for its duration in its terms (high protection).
Justification of answer	Unilateral changes are possible but at least 30 days prior notification is possible. Given that the counterparty can at all times terminate within this timeframe without reason, the counterparty can get out of the contract and has a reasonably long time to find another solution.

Control	**This control relates to the terms in the contractual documents provided by the CSP in relation to the determination of liability, and, specifically the limitations of liability that are present, looking at the level of protection offered to the CSP's counterparty.**
Question (for the legal expert)	Taking into account all terms in the contractual documents, what is the level of protection offered to the CSP's counterparty in terms of options to recover damages, taking into account the extent to which liability is limited?
Possible answers	There is no option. All liability is excluded, even contra legem.
	There are theoretical options to recover damages but they are heavily limited and it is questionable that in reality the CSP's counterparty will be able to obtain a reasonable measure of redress, e.g. because of far-reaching carve-outs or a very restrictive liability cap (reservation) (low protection).
	There are options to recover damages, although limited in a reasonable way and according to industry practice. Redress is reasonably obtainable but may be limited in amount (medium protection)
	There are reasonable and balanced options to recover damages. Limitations are either not present or favourable for the CSP's counterparty (high protection).
Justification of answer	Liability is limited to amounts paid in the previous month and only recoverable in credits. Moreover, there are some extensive carve-outs leading to any liability scenario being more theoretical than real, certainly also taking into account the force majeure clause.
Control	**This control relates to the contractual definition of force majeure, which prevents any liability from arising at all. The conditions under which force majeure is considered to be present may be another way for the CSP to limit it's liability towards the counterparty.**
Question (for the legal expert)	Taking into account the contractual terms on force majeure, how do you assess the remaining level of protection for the CSP's counterparty, taking into account that, while force majeure is a reasonable exception in itself, an overly extensive interpretation may create a backdoor for the CSP to unduly escape liability?
Possible answers	Force majeure is interpreted so extensively that no liability can ever exist.
	Force majeure has a (very) extensive interpretation, posing a real risk of hollowing out any liability possibility, which will likely lead to discussion if certain events arise (reservation) (low protection).

	Force majeure is described in a reasonable manner and does not principally hollow out liability (medium protection)
	Force majeure is described clearly and precisely and is limited to classic force majeure scenarios (high protection).
Justification of answer	Extensive clause, further hollowing out the liability scenarios.
Control	**This control relates to the contractual provisions on confidentiality, other than the confidentiality obligations under Article 28 GDPR, but rather in more general terms.** **The focus of the control is first on the fact that confidentiality should be comprehensive and the obligation clear and enforceable. Typically, confidentiality applies to both Parties equally, but if not, the focus would be on the CSP's part of the obligation.**
Question (for the legal expert)	What is the level of protection offered by the text of the general confidentiality obligations resting on the parties, specifically on the CSP?
Possible answers	No confidentiality is guaranteed.
	Basic references are available to confidentiality but faulty and/or incomprehensive, and/or enforcement problems to be expected (reservation) (low protection).
	There is a clear and enforceable confidentiality obligation for both Parties (medium protection).
	Confidentiality obligations are clear and enforceable and are fully comprehensive (high protection).
Justification of answer	The confidentiality clause is the same for both parties, clear and reasonable. It lacks some detail and hence is medium protection only.

Result matrix and assigning a legal level to the service

Table 10. Example 1 (SME CSP Cloud service) result matrix for the legal level

Control	Result
Simple controls that are applicable	
Valid company registration	✓
DPO/data protection point of contact	✓
Data processing agreement (DPA)	✓
ISO 27001 or equivalent	✓
Cloud certification covering all CCSM objectives	×
Adherence to Data Portability and Switching Code of Conduct	×
Adherence to Data Protection Code of Conduct	×
Layered controls that are applicable	
Termination options of CSP's counterparty	★★
Liability coverage	★
Force majeure coverage	★
DPA scope	★★★
Documented instructions only	★★
DPA confidentiality	★★★
CSP security A32 GDPR	★★★
Sub-processor engagement	★★
Contractual pushdown sub-processor	★★★
Sub-processor liability coverage	★★★
Data subject request assistance	★★
Counterparty security measures assistance	★★
Data breach notification assistance	★★★
DPIA assistance	★★

Control	Result
Deletion or return of data	★★★
Compliance information obligation	★★
Audit rights granted	★★
Illegal instructions notification obligation	★★★
DPA liability coverage (if relevant)	★★
Termination possibilities DPA (if relevant)	★★★
Termination/suspension options CSP	★★
Limitation of unilateral changes by CSP	★★
Confidentiality terms (general)	★★

When comparing this with the legal level matrix, and taking into account that:

- All controls that were not relevant are not taken into account; and
- A service only gets the tier of legal level for which it meets ALL the requirements;

The result of for this service is: tier 2 (substantial legal safeguards).

This is because:

- It meets all requirements of tier 2 for simple controls, but not more and certainly not the requirements for tier 1. Hence it can maximum be tier 2.
- It meets all requirements for tier 2 for the layered control and for some even more. However, it does not meet all requirements for tier 1, nor in layered controls, nor in the simple controls, as described above.

2.8.2 Example 2: selected large CSP Cloud service

Simple controls

Question to the CSP	Answer
Is your organization a validly registered and incorporated entity, which is neither in liquidation nor in a state of bankruptcy?	Yes
Did your organization appoint and will it maintain a DPO in accordance with Articles 37-39 of the GDPR or an equivalent position e.g. a privacy officer or privacy team which can act as a data protection point of contact?	Yes
Do you provide a data processing agreement which is compliant with Article 28 of the GPDR?	Yes

Question to the CSP	Answer
Did your organization obtain and does it maintain a certification under the ISO 27001 standard or equivalent, covering the service in question?	Yes
Did your organization obtain and does it maintain at least one certification that meets all of the 27 security objectives of the Cloud Certification Schemes Metaframework as defined by ENISA, such as CSA attestation/certification – OCF level 2, TÜV Rheinland Certified Cloud Service certification or equivalent and which covers the service in question?	Yes
Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting reasonable industry standards for data portability and switching as intended by Article 6 of the Regulation on the free flow of data?	No
Does your organization adhere to at least one self-regulatory instrument (code of conduct) setting out data protection requirements, approved under Article 40 GDPR?	No

Layered controls

Control	**Adequacy of the scope description in the DPA, as required by Article 28(3) GDPR.**
Question (for the legal expert)	How would you assess the description of subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects as required by Article 28(3) GDPR in the DPA under revision?
Possible answers	Description not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clause is present, but description of scope is rather limited.
Control	**Adequacy of the contractual obligation for the CSP as a (sub-) processor to process personal data, including with regards to data transfers outside the EEA, only on the documented instructions of the CSP's counterparty, as prescribed by Article 28(3), a) GDPR, unless required to do so by EU or member state law, in which case the CSP has to inform its counterparty of that legal requirement, unless that in itself is forbidden by the legal rule in question.**

Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP as a (sub-)processor to only act on the documented instructions of the CSP's counterparty, in the light of Article 28(3), a) of the GDPR and the current official interpretation available?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clause is present with clear description, but there are caveats and the instructions are defined by reference.
Control	**Adequacy of the contractual obligation for the CSP to ensure confidentiality of personnel and agents authorized to process data on its behalf through commitments of confidentiality or by the relevant persons being under a statutory obligation of confidentiality, as prescribed by Article 28(3), b) GDPR.**
Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP to ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation) (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clause is present but very general and rather limited.
Control	**Adequacy of the contractual obligation for the CSP to take the appropriate technical and organizational measures to ensure a level of security appropriate to the risk, pursuant to Article 32 GDPR, as prescribed by Article 28(3), c) GDPR.**

Question (for the legal expert)	How would you assess the description in the DPA of the obligation for the CSP to take all security measures pursuant to Article 32 GDPR, in the light of the obligation of Article 28(3), c) GDPR to include a clause detailing such measures in the DPA?
Possible answers	Obligation not present.
	Present, but potentially faulty (e.g. making the controller agree that a certain set of current measures will forever be appropriate) or unclear description given the context of the given CSP (reservation), so that it may be insufficient under Article 28(3), c) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), c) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	The obligation is open-ended and general, so the CSP's counterparty is not bound to accept a given set of measures as sufficient, which would be negative. The contractual documents do give examples of measures taken and some of the potential measures that the customer may request. The description of some of the measures however could be better. r
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the engagement of sub-processors by the CSP, specifically the need to have prior general or specific written authorization, and, in the case of general authorization, to inform its counterparty of intended changes, offering its counterparty an opportunity to object to such changes, as prescribed by Article 28(3), d) and 28(2) GDPR.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(2) GDPR, as referred to in Article 28(3), d) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonably short delays, an infeasible manner of objection, or other conditions arguably hollowing out the legally intended effect of Article 28(2) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).

Justification of answer	There is a general written consent but with prior notification of at least 30 days. Customers may object and move data to a region not covered by the new sub-processor or may terminate the agreement.
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the consequences of engaging a sub-processor, namely that the same data protection obligations binding the CSP to the CSP's counterparty should be passed down to the sub-processor of the CSP, as prescribed by Article 28(3), d) GDPR and Article 28(4) GDPR.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with the requirement of pushing down the same data protection terms binding the CSP on any sub-processors engaged in the processing by the CSP, as described in Article 28(4) GDPR, as referred to in Article 28(3), d) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential limitations or obscurity created by the contract terms which may be interpreted as such, arguably hollowing out the legally intended effect of Article 28(4) GDPR. (Low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	The contract specifies they will push down the exact same terms. There is a carveout which doesn't seem to impact the result.
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the consequences of engaging a sub-processor, namely that there should be a clear affirmation that the CSP shall in any case remain liable towards the CSP's counterparty for failure of its sub-processor to perform its obligations, as prescribed by Article 28(3), d) GDPR and Article 28(4) GDPR.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(4) GDPR, as referred to in Article 28(3), d) GDPR, namely that there should be a clear statement that the CSP will always remain liable towards its counterparty if the CSPs sub-processor fails to fulfil its obligations?
Possible answers	Obligation not present.

	Present, but potentially faulty or unclear description (reservation), e.g. because of potential limitations or obscurity created by the contract terms which may be interpreted as such, arguably hollowing out the legally intended effect of Article 28(4) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), d) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Wording of this provision seems to exclude some situations from liability coverage. This would make it a hollowing out of the intended effect of Article 28(4).
Control	**This control relates to the adequacy of the contractual obligation in the DPA in relation to the CSP assisting its counterparty, by appropriate technical and operational measures insofar as this is possible, to respond to data subject requests, as prescribed by Article 28(3), e) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including those relating to cost and conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA to provide compliance with Article 28(3), e) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of high costs, unreasonable conditions or other, arguably hollowing out the legally intended effect of Article 28(3), e) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), e) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	The contract specifies that in the UI there are sufficient controls for this and that the CSP when contacted by a data subject will use commercially reasonable efforts to forward the request to the counterparty. While indeed certain tools may be presented as a first option to fulfil such assistance and while imposing certain conditions or limitations is generally possible, this hollows out the assistance obligation since customer would have to go negotiate for assistance outside what is provided “as is” as tools. While this may not be a big problem in practice, in legal terms, it is faulty.

Control	**This control relates to the adequacy of the contractual obligation in the DPA with regards to the CSP's obligation to assist its counterparty in attaining an adequate level of security of processing as meant in Article 32 GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including those relating to cost and conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide assistance to its counterparty in the counterparty's own obligation to ensure an adequate level of security of processing, as required by Article 28(3), f) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of high costs, unreasonable conditions or other, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Again the contract only provides that some extra security tools and features may be obtained by the CSP's counterparty to aid in its own security obligation. No other assistance is offered, not even ad hoc or subject to limitations and against payment. Hence this seems to hollow out the purpose of this obligation under the GDPR.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to support its counterparty with the latter's obligation to notify the supervisory authority and/or the data subject in case of a data breach, likely to result in a (high) risk for data subjects, as provided in Article 28(3), f) GDPR, 33 GDPR and 34 GDPR. It assesses the content of that obligation in the DPA and its potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide support in fulfilling the notification obligations of Article 33 and 34 GDPR as required by Article 28(3), f) GDPR, specifically outside the own processor-specific obligation to notify the controller without undue delay after becoming aware of a data breach (Article 33(2) GDPR)?

Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clear obligation to report without undue delay, but carveouts in assistance obligations (although reasonable) and in the type of security incidents to be reported lead to this being less than fully adequate, and hence medium protection.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to support its counterparty with the latter's obligation to carry out a data protection impact assessment (DPIA) on intended processing activities that meet the requirements set by Article 35 GDPR (likely to result in a high risk for the data subject) and to consult with a supervisory authority prior to carrying out the planned processing activity when the outcome of the data protection impact assessment is that there is a high residual risk, despite the risk containment and prevention measures already taken by the counterparty and detailed in the DPIA, i.e. that there is a high risk remaining in the absence of further controlling measures to be taken by the controller (Article 36 GDPR). It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities of such assistance, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to provide support in fulfilling its counterparty's obligation to carry out a data protection impact assessment under the conditions provide in Article 35 GDPR and, where applicable, of the prior consultation obligation contained in Article 36 GDPR, as required by Article 28(3), f) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, unreasonably high costs, lack of capacity of the counterparty to decide when a data protection impact assessment or prior consultation is necessary, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), f) GDPR (low protection).

	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), f) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Present but merely by reference to making audit reports available on request. This is a very limited interpretation of the obligation in question and may very well not hold in court. The exclusion of any other kind of assistance, even against payment, seems to hollow out the obligation to a considerable extent.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to delete or return, at the choice of its counterparty, all personal data of the controller at the end of the contract, unless EU or member state law specifically requires further storage of that data, as defined in Article 28(3), g) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	Taking into account all the contracts terms (or their absence) on this point, including any conditions/modalities, how do you assess the adequacy of the contractual obligation in the DPA for the CSP to, a the choice of the counterparty, delete or return all personal data to the counterparty at the end of the provision of services?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), g) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), g) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Clause provides CSP's counterparty with the choice to retrieve data or have it deleted using controls provided in the UI, during an extensive period, unless prohibited by law, the order of regulatory or governmental body or when it would expose the CSP to liability. This limitation is not necessarily an issue, but there is no specification of what happens to the data in such a case. Moreover, some unclarity exists for several other scenarios: what happens to the data if retrieved is it retained by the CSP? And what happens when the Counterparty does not use the controls provided? All in all the clause is likely to be considered compliant, but could still is more precise. Hence medium protection.

Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to provide its counterparty with all compliance information necessary, specifically to show the CSP's compliance with the obligations defined by Article 28, as defined in Article 28(3), h) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP to make available to its counterparty all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), h) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), h) GDPR (medium protection).
	Present and fully adequate (high protection).
Justification of answer	Present, but the information is limited to a couple of pre-identified documents, mostly relating to information security measures and management. While this is highly relevant, the obligation should be broader and extend to all information that the CSP's counterparty could require ascertaining compliance under Article 28 GDPR. In the current wording, the CSP's counterparty has to hope the provided documentation will clarify all questions the counterparty may have.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to allow for and contribute to audits, including inspections either carried out by the counterparty itself or by another auditor mandated by the counterparty, as required explicitly by Article 28(3), h) GDPR. It assesses the content of that obligation in the DPA, specifically looking at potential conditions, limitations and requirements.**
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP submit itself to audits, including inspections carried out by the counterparty itself or by another auditor mandated by the counterparty, as required by Article 28(3), h) GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of unreasonable conditions (high costs, long delays, etc.),

	carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), h) GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), h) GDPR (medium protection).
	Present and fully adequate, providing for real audit and inspection rights at reasonable conditions for the counterparty (high protection).
Justification of answer	Obligation present but completely hollowed out by replacing the right to audit with a CSP audit, the report of which can be accessed by the CSP's counterparty on request and provided there is an NDA. A customer audit is supposed to give the CSP the instruction to carry out the standard audit already carried out by the CSP. The counterparty can change this instruction by written notice only and the CSP can deny, at which point the counterparty is however entitled to terminate the contract and the DPA. Nonetheless, this hollows out the obligation of Article 28(3), h). Hence low protection.
Control	**This control relates to the adequacy of the contractual obligation in the DPA for the CSP to immediately inform the counterparty if any of its instructions are, in the opinion of the CSP, contrary to applicable data protection law (GDPR, EU law or member state law).**
Question (for the legal expert)	How do you assess the obligation in the DPA obliging the CSP to immediately inform the counterparty if it considers any of the counterparty's instructions contrary to applicable data protection law as required by Article 28(3), second subparagraph GDPR?
Possible answers	Obligation not present.
	Present, but potentially faulty or unclear description (reservation), e.g. because of potential delays, carveouts or other faults, arguably hollowing out the legally intended effect of Article 28(3), second subparagraph GDPR (low protection).
	Present and adequate enough so that it is unlikely to be legally challengeable under Article 28(3), second subparagraph GDPR (medium protection).
	Present and fully adequate (high protection).
Justification	Obligation follows from conjunctive reading of provisions. Obligation should be more clear, explicit and precise.
Control (if relevant)	**This control addresses the termination clause of the DPA, if there is any. Such a clause is not obligatory but if present must not limit the effect of the DPA. In practice such clauses are nonetheless found and they have**

	the effect of hollowing out the intended effect of article 28 GDPR. This control aims to assess this potential threat. **Note: If no clause is present, this control is not considered, since it cannot in general terms be stated whether or not this is a positive or a negative point.**
Question (for the legal expert)	If there is a termination clause in the DPA, does it ensure protection of the CSP's counterparty and compliance under article 28 GDPR?
Possible answers	No, the DPA can easily be terminated, leaving the service contract of the services that contain the processing activities intact, without a valid DPA.
	This is unclear, the wording of the contract is vague or faulty, or there is a reference which does not contain specific language on this topic; it could reasonably be questioned whether this clause has the effect of hollowing out Article 28 GDPR (reservation) low protection.
	The DPA's termination clause is reasonably formulated and to be interpreted as logically following the main service agreement; it is unlikely to be interpreted as hollowing out Article 28 GDPR (medium protection).
	The DPA's termination clause is clearly worded and leaves no or little room for misinterpretation. The DPA logically follows the main contract. It is very likely compliant with the GDPR and does not hollow out Article 28 GDPR (high protection).
Justification of answer	Clear clause, no discussion possible.
Control	**This control assesses the level of the contractual possibilities to terminate the contract with the CSP. It aims to measure how flexibly the counterparty of the CSP can get out of the contract. Some termination possibilities are standard, e.g. for material breach. Others are not. Some CSPs offer very flexibly terminated contracts, while others strictly limit this, through a variety of clauses, including through the manner in which notification can be given. The consequences of termination are also taking into account.**
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms, how do you assess the level of ease offered to the CSP's counterparty in terminating the contract in a situation where the CSP's services are no longer wanted, also taking account of any consequences of termination?
Possible answers	There are unreasonable punitive clauses, limitations and exceptions or otherwise clauses which make termination very difficult.

	Termination is possible, but only in limited circumstances e.g. breach of contract, or with a very early prior notice, or under conditions which are substantially aimed to protect the CSP (reservation) (low protection)
	Termination is possible in most or all circumstances, notice periods are reasonable if any and the conditions are reasonably balanced, termination is also possible without notice under breach of contract, although grace periods may apply. (medium protection)
	Termination is very easy and always possible. No notice period applies or it is very limited. Breach of contract justifies immediate termination with little grace periods, if any. All conditions are favourable to the CSP's counterparty (high protection).
Justification of answer	Termination is always possible for the counterparty. Termination without notice is possible when the CSP is in breach of contract. Termination consequences are reasonable.
Control	**This control assesses the options available to the CSP to terminate or suspend the contract and the resulting level of protection of the CSP's counterparty in continuity of the enlisted services.**
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms, how do you assess the level of protection offered to the CSP's counterparty when looking at the options available to the CSP to terminate or suspend the contract.
Possible answers	There is no protection. The CSP can terminate and/or suspend at will, with no reason or notice and there are no mechanisms to ease the transition.
	Termination and/or suspension is very easy for the CSP, many options being available with a low threshold, including options for termination/suspension without notice based on very low-threshold contractual shortcomings of the counterparty (reservation) (low protection)
	Termination and/or suspension are possible in several circumstances, but there are notice periods and/or other mechanisms to ease transition and this is reasonable. Termination/suspension without notice is only possible on the basis of reasonable conditions (medium protection).
	Termination and/or suspension are possible in a reasonably limited number of circumstances. Notice periods and/or other mechanisms to ease transition are favourable to the CSP's counterparty. Termination/suspension without notice is strictly limited (high protection).
Justification of answer	Notice period for the CSP is 30 days. Suspension is possible only in certain circumstances, but some circumstances are potentially low threshold and

	any suspension also warrants termination by the CSP without notice. Termination for cause (breach of contract) is possible in limited circumstances, but one is potentially low threshold and another does not actually constitute cause. Hence, since there are some shortcomings but nothing major, medium protection.
Control	**This control assesses whether or not, and to what extent the CSP is reserving the right to unilaterally change the contractual documents. This is a provision often found in CSP contracts and may be an issues if the changed terms are unacceptable for the user. The way in which this is done and the period of notice are relevant factors to take into account. The control is measuring the level of protection for the CSP's counterparty, and thus more flexibility for the CSP means less protection in terms of guaranteed continuity for the CSP's counterparty. The absence of such a clause, which implies that the contract is permanent and more durable, is a positive point. In a way, this is the other side of the coin of the control on ease of termination for the CSP's counterparty.**
Question (for the legal expert)	Taking into account the nature of the Cloud services (bespoke vs. generic) and all relevant contractual terms how do you assess the level of protection offered to the CSP's counterparty from potentially disruptive unilateral changes of contract?
Possible answers	Unilateral changes are possible, without the CSP having to give a reason, and with very little to no notice period, giving the CSP's counterparty little to no time to find alternatives if the new terms are unsuitable.
	Unilateral changes are possible, without the CSP having to give a reason, and with a short notice period, giving the CSP's counterparty some opportunity to find alternative solutions if the new terms of the contract are unsuitable (reservation) (low protection).
	Unilateral changes are possible, with or without the CSP having to give a reason, but there is a reasonable notice period and potentially other mechanisms giving the CSP's counterparty a fair opportunity to find alternative solutions if the new terms of the contract are unsuitable (medium protection).
	Unilateral changes are not possible. The contract is fixed for its duration in its terms (high protection).
Justification of answer	Unilateral changes are possible at all times. 90 days advance notice is given, but only for SLA's and only if the changes are considered adverse for the CSP's counterparty. Hence, the low protection, since many changes are not covered, while they may still be relevant.
Control	**This control relates to the terms in the contractual documents provided by the CSP in relation to the determination of liability, and, specifically**

	the limitations of liability that are present, looking at the level of protection offered to the CSP's counterparty.
Question (for the legal expert)	Taking into account all terms in the contractual documents, what is the level of protection offered to the CSP's counterparty in terms of options to recover damages, taking into account the extent to which liability is limited?
Possible answers	There is no option. All liability is excluded, even contra legem.
	There are theoretical options to recover damages but they are heavily limited and it is questionable that in reality the CSP's counterparty will be able to obtain a reasonable measure of redress, e.g. because of far-reaching carve-outs or a very restrictive liability cap (reservation) (low protection).
	There are options to recover damages, although limited in a reasonable way and according to industry practice. Redress is reasonably obtainable but may be limited in amount (medium protection)
	There are reasonable and balanced options to recover damages. Limitations are either not present or favourable for the CSP's counterparty (high protection).
Justification of answer	Liability is limited to amounts paid in the previous year (but only for the CSP, the counterparty's liability seems unaffected), but there are a great many carveouts, leading liability scenarios to be quite limited.
Control	**This control relates to the contractual definition of force majeure, which prevents any liability from arising at all. The conditions under which force majeure is considered to be present may be another way for the CSP to limit it's liability towards the counterparty.**
Question (for the legal expert)	Taking into account the contractual terms on force majeure, how do you assess the remaining level of protection for the CSP's counterparty, taking into account that, while force majeure is a reasonable exception in itself, an overly extensive interpretation may create a backdoor for the CSP to unduly escape liability?
Possible answers	Force majeure is interpreted so extensively that no liability can ever exist.
	Force majeure has a (very) extensive interpretation, posing a real risk of hollowing out any liability possibility, which will likely lead to discussion if certain events arise (reservation) (low protection).
	Force majeure is described in a reasonable manner and does not principally hollow out liability (medium protection)

	Force majeure is described clearly and precisely and is limited to classic force majeure scenarios (high protection).
Justification of answer	Extensive clause, further hollowing out the liability scenarios.
Control	**This control relates to the contractual provisions on confidentiality, other than the confidentiality obligations under Article 28 GDPR, but rather in more general terms.** **The focus of the control is first on the fact that confidentiality should be comprehensive and the obligation clear and enforceable. Typically, confidentiality applies to both Parties equally, but if not, the focus would be on the CSP's part of the obligation.**
Question (for the legal expert)	What is the level of protection offered by the text of the general confidentiality obligations resting on the parties, specifically on the CSP?
Possible answers	No confidentiality is guaranteed.
	Basic references are available to confidentiality but faulty and/or incomprehensive, and/or enforcement problems to be expected (reservation) (low protection).
	There is a clear and enforceable confidentiality obligation for both Parties (medium protection).
	Confidentiality obligations are clear and enforceable and are fully comprehensive (high protection).
Justification of answer	The confidentiality clause mostly refers to confidentiality owed to the CSP; the responsibilities of the CSP are much less clear. Low protection.

Result matrix and assigning a legal level to the service

Table 11. Example 2 (large CSP Cloud service) result matrix for the legal level

Control	Result
Simple controls that are applicable	
Valid company registration	✓
DPO/data protection point of contact	✓
Data processing agreement (DPA)	✓
ISO 27001 or equivalent	✓

Control	Result
Cloud certification covering all CCSM objectives	✓
Adherence to Data Portability and Switching Code of Conduct	✗
Adherence to Data Protection Code of Conduct	✗
Layered controls that are applicable	
Termination options of CSP's counterparty	★★★
Liability coverage	★
Force majeure coverage	★
DPA scope	★★
Documented instructions only	★★
DPA confidentiality	★★
CSP security A32 GDPR	★★
Sub-processor engagement	★★★
Contractual pushdown sub-processor	★★★
Sub-processor liability coverage	★
Data subject request assistance	★
Counterparty security measures assistance	★
Data breach notification assistance	★★
DPIA assistance	★
Deletion or return of data	★★
Compliance information obligation	★
Audit rights granted	★
Illegal instructions notification obligation	★
Termination possibilities DPA (if relevant)	★★★
Termination/suspension options CSP	★★

Control	Result
Limitation of unilateral changes by CSP	★
Confidentiality terms (general)	★

When comparing this with the legal level matrix, and taking into account that:

- All controls that were not relevant are not taken into account; and
- A service only gets the tier of legal level for which it meets ALL the requirements;

The result of for this service is: tier 3 (basic legal safeguards).

This is because:

- It meets all requirements of tier 3 for simple controls. It also meets additional requirements, including all the requirements for tier 2 but not all the requirements of tier 1.
- It meets all requirements for tier 3 for the layered control and on several aspects scores much better than the baseline requirement of 1 star. However, it does not meet all requirements for tier 2 in layered controls. Hence, the highest level that can be assigned is tier 3.

2.9 Use cases for the legal level

This section presents some use cases showing how the legal level may be used by certain target user organizations as a useful non-functional requirement of the multi-Cloud application to pre-select (and pre-reject) Cloud services, enlisting only Cloud services in the deployment that fit its identified legal needs.

In D5.3, it was presented already that the legal level is meant to translate the legal requirements, compliance burden, risk appetite and even business complexity (type of data processed, scale) into an easy-to-use and easy-to-understand legal level, consisting of three tiers.

It was stated, roughly, that the following correspondence would be present between the tier of the legal level and the organizations/projects/applications for which the tier might be best suited:

Table 12. Abstract recommendations for the use of the legal level

Legal level tier	May be suited for which organizations/projects/applications
Legal level tier 3 (basic legal safeguards)	May be best suited for non-data driven organizations or projects/applications with limited data and no sensitive data, low compliance risk or higher risk appetite and limited business complexity. Examples may include non-data driven start-ups and SMEs and larger companies dealing mostly with non-personal data (heavy industry, manufacturing).
Legal level tier 2 (substantial legal safeguards)	May be best suited for organizations or projects/applications with average data processing activities, which may process large amounts of personal data but not large amounts of sensitive data or special categories of data. Examples may include data-driven

	companies working with personal data but not sensitive data/special categories of data. Governmental entities treating largely non-sensitive data may also choose this level, unless there are requirements in place for the use of cloud services which are not reflected in tier 2.
Legal level tier 1 (strong legal safeguards)	May be best suited for organizations or projects/applications which have a low risk appetite and higher compliance risks/burden because of the type of data processed (e.g. health data, financial data) or because of the sector in which they are active, adding regulatory requirements to the mix. Examples include health professionals and hospitals, banks, and governmental organizations which also treat sensitive data.

While this remains true, it is only a rough indication of what legal level tier might be suited for a given organization, project or application.

Choosing the correct legal level tier will always depend on the situation at hand, and thus, is not possible to be accurately performed in an abstract manner.

It remains up to the target user organization to determine what legal level tier they need, depending on the situation at hand. That is why the merely matrix specifies what every tier offers, while trying not to assign weight other than in an abstract manner, so that importance can be assigned by the target user organization and the legal level tier be chosen accordingly. The legal level is offered “AS IS” and no guarantees are made as to its effectiveness and usefulness. This is also why ACSmI offers no specific recommendations either. Such a service may however be offered (ad hoc) by DECIDE partners as part of the DECIDE exploitation plan.

For now, however, target user organizations, in fact through the application developer who will need to assess the needs of the target user organization(s), will need to determine which legal controls are most relevant to them, what level of assurance they want (for simple controls present/not present, for layered controls 1, 2 or 3 stars), and what legal level tier corresponds to those needs.

For general commercial entities, this assessment may be done purely internally. Entities in regulated sectors and governmental entities may additionally have to take into account regulatory requirements and/or guidelines and thus may be forced to take a higher tier of the legal level because of those requirements. Generally, the legal level tier will be determined by the most important requirements of a target user organization. This is because of the way the legal level has been conceptualized.

If several important layered controls for example require medium protection for a given application, legal level tier 2 will be the first tier to satisfy these requirements. If only one of those controls however requires (e.g. because of a regulatory requirement) a level of high protection, which is only found in tier 1, the whole application will need to be deployed with Cloud services offering tier 1 high protection.

This may seem unnecessary as this will entail many other controls also being at a level of high protection whereas the target organization’s needs do not require this. This is however unavoidable when assigning tiers of legal level in a general way, or in other words, dividing services into three categories in a general way. By making a generally applicable division of services based on the legal protection offered, it is necessary to make a division in some way and to define thresholds, which, once crossed from the CSP’s side, lead to the inclusion of the service in another category. The

consequence of this is that, from the target user organization's point of view, there may be a need to go to a higher tier in order to obtain some specific level of protection in one or a few controls, which is not offered by the tier below. When crossing this threshold from one tier into another, the level of protection offered by the controls will change significantly, i.e. most controls will offer a higher level of protection, not just the relevant ones. Since the legal level matrix and the different tiers are defined in a general way and not customized to the target user organization or the sector, crossing the tier threshold and changing legal tiers because one or a few control(s) needs a higher level, will have a collateral impact on the other controls.

This should not be too much of a concern however, as the legal level errs on the side of too cautious in this scenario (it gives more guarantees) and it is not been established that the legal level actually has a correlation with the price of the service (it weeds out only the Services that do not meet the legal level, but these are not necessarily cheaper), so the target user organization may not necessarily pay more for this and may actually be getting more value for money.

However, acknowledging this inherent problem of lack of granular customization of the legal level, section 5 already mentions the future possibility to have custom made legal levels or legal levels per sector (e.g. if for banks audit requirements are important, their tier 2 can contain a high level of protection for this control already), where the legal level can move from the general and abstract to the more individual/customized and precise, which will make its function as non-functional requirement used to pre-select (and pre-reject) possible Cloud-services through the DECIDE framework more accurate and valuable.

Notwithstanding the foregoing, **this section aims to present a few use cases in which the value of the legal level is shown.** This value is already present in the current abstract and general form. It may however be multiplied in the future through further granular customization.

Four use cases are defined:

- First, a general commercial use case is defined, containing several hypothetical examples. It serves to illustrate why companies may for commercial reasons decide on one tier of the legal level or another.
- The second use case relates to the banking sector. Financial institutions and payment institutions are subject to extensive (EU-level) regulation outsourcing tasks and/or activities are regulated as well. There are specific rules on the use of Cloud services and thus this is an interesting use case to look at, showing that also in a heavily regulated industry the legal level may have value.
- The third use case relates to healthcare. Healthcare is interesting because it processes special categories of data (data relating to health), as defined in Article 9 of the GDPR. Moreover, healthcare is also intensely regulated (on the national level). The use case highlights the facilitating role the legal level may play in such an environment.
- The fourth use case relates to the use of Cloud services in e-government.

2.9.1 Use case: general commercial use

Before discussing specific cases in specific and/or strongly regulated environments, it is worth briefly considering the use of the legal level in general commerce, i.e. by diverse companies in other sectors than those considered in the next use cases.

The legal level can easily translate the company's requirements with regards to legal protection into a non-functional requirement for its multi-Cloud application, thereby automatically only proposing services that match:

- The company's compliance burden
- The business complexity
    - Type of data processed
    - Scale
    - Data driven or not
    - Start-up (perhaps even pre-commercial) vs. established
    - Customer expectations
- The company's risk appetite

The following table contains some fictitious examples that illustrate how the legal level can be helpful.

Table 13. Examples of general commercial use of the legal level

Scenario	Recommended tier	How the legal level helps
Company A provides asset management services to an elite clientele. They want to host their bespoke software in the Cloud but want to ensure and showcase GDPR compliance of the multi-Cloud native solution.	Tier 1 (strong legal safeguards)	The legal level helps to ensure that the contracts offered by the CSP(s) offer high protection. Moreover, this function can be showcased to clients.
Company A has identified that it acts as a processor for its clients. It promises rather client-protective terms to its clients because it sees this as a matter of good service.	Tier 1 (strong legal safeguards)	Under Article 28(4), company A will as a first processor remain liable for all CSP failures. In principle it also needs to push down the DPA terms with its customers to the CSPs. While this will not be possible, selecting tier 1 CSPs only will help remedy the liability risk that company A has taken here.
Company B is active in manufacturing of heavy industry equipment. They want to run an internal system which deals exclusively with non-personal machine data on multi-Cloud infrastructure. Company B does not specifically care about GDPR compliance as they have identified no personal data to be involved. They do not particularly care with which CSP the system is hosted and confidentiality is not a major concern.	Tier 3 (basic legal safeguards)	Company B has basic requirements when it comes to legal matters. They want a basic solution that offers the essentials. Hence tier 3 of the legal level will suffice.

Scenario	Recommended tier	How the legal level helps
Company B realizes the data in their system actually reveals important information about how they conduct their business. The legal department worries about the confidentiality of that information in the public Cloud.	Tier 2 (substantial legal safeguards) or higher	Of course company B could opt for another option (e.g. private Cloud), but it could also adapt the legal level of any CSPs used to tier 2 or even tier 1. This guarantees that the confidentiality clauses in the contract are enforceable, balanced and not subject to conditions or carveouts.
Company B decides to add operator information to their machine data. Their legal department warns them that this will lead to the database being requalified as personal data under the GDPR. Moreover, as their current CSPs are mostly based in the US (since they are the cheapest); they worry about the legal compliance.	Tier 3 (basic legal safeguards) or higher	By making their database contain personal data, company B enters the scope of the GDPR with this activity. Hence it becomes important to ensure that certain measures are present, such as a DPA, a data transfer mechanism etc. Tier 3 already provides this and thus the company could stick with tier 3. However, the content of the contractual documents on this point is also of relevance. While tier 3 may already guarantee the presence of such measures, it does not guarantee much in terms of content. Hence, the company may want to go a tier higher to ensure at least a medium level of protection on the many controls related to data protection. This helps ensure company B's compliance. As company B is the controller and does not have to carry the risk as a processor against a controller for its sub-processors, it may want to take the approach that mere presence of GDPR documents is enough and stick to tier 3. Hence, tier 2 or tier 3 depends on the risk appetite and the management approach of company B, but it should help the company easily and safely translate that policy into the selection of its Cloud services.
Company C is a fintech start-up. It has developed a multi-Cloud native payment app, hosted on external Cloud infrastructure. The app has not officially been launched and only has a limited and controlled user	Tier 3 (basic legal safeguards) or higher	While financial data is personal data and may also warrant a more risk-averse approach to selecting CSPs (i.e. a higher legal level), a start-up which is pre-commercial may not need all those guarantees.

Scenario	Recommended tier	How the legal level helps
base and most data used for tests and development is fake data.		
Company C decides to launch its product commercially. It also has to obtain a license for this with the supervisory authority, which i.e. imposes stringent audit requirements on company C as to the security of the product.	Tier 1 (strong legal safeguards)	Because company C's external legal situation has changed, they now need more guarantees from the CSPs in order to satisfy their changed legal needs. E.g. for the audit requirement to be satisfied, they need to assure that the CSPs they use, offer an appropriately strong audit guarantee. Hence tier 1. Please note that the legal level alone may not be enough in cases of regulated sectors. Refer to the other use cases for this.
Company D is a start-up which is making a tool to better compare local service suppliers in a variety of services. To enable this, contact details of service suppliers are necessary, as well as verified reviews by clients. The company starts with open data sets and aims to add reviews and other information through the CEO's wide network. When obtaining the open data, company D learns that the open data licence specifies rather stringent security requirements. In fact, it seems that a verified level of information security management is required to obtain the otherwise free datasets. Company D aims to handle that data and run the tool on external (multi-)Cloud infrastructure.	Tier 2 (substantial legal safeguards)	In this case, company D should have security measures in place but importantly should also verify that the CSPs used have this. Hence it would be a good move to require the CSPs to have ISO27001 certification or equivalent. Taking tier 2 provides for this. Moreover, as personal data will be involved, it would be wise to get a higher level of DPA protection than what is provided by tier 3.
When developing the tool, company D decides it wants to link the reviews it is gathering to demographic data of the reviewers, to better tailor the functioning of the tool to the user, who, when registering from now on would also have to provide a set of information. Before implementing this measure, company D wants to conduct a	Tier 2 (substantial legal safeguards) or higher	This is a classic example of how a CSP might be involved in a DPIA. In this case it is important that an assistance obligation exists (tier 3), but also that it is adequate and balance, so that there are no extreme or unreasonably high costs or other conditions which the CSP could use to frustrate the DPIA's process. Hence, tier 2 or higher, guaranteeing a decent obligation on

Scenario	Recommended tier	How the legal level helps
DPIA. However, when trying to define the security measures in place, company D has to turn to the CSP.		this end, as well as assistance with any data subject requests that may for example follow and where the CSP's help should be needed (probably only in rare cases where the provided controls in the UI do not suffice).
Company E is making a multi-cloud native e-health app. The app is still being developed and no real data is being processed yet. However, company E wants to ensure that the CSPs used provide a high level of security and do not stand in the way of company E providing its users a strong measure of control over their data, which is considered a selling point and a threshold-lowering measure for people to install and use the app.	Tier 1 (strong legal safeguards)	Important here is that the DPA obligations should be of a high level, including Art. 32 GDPR security, assistance with data subject requests and deletion/return of data. Also, the adherence of the CSP to code of conducts is relevant and the certifications present help ensure a level of security at the CSP. Audit rights may be very relevant too for company E to verify this. Hence, choosing legal level tier 1 Cloud services only will help make managing their multi-Cloud solution much easier for company E.
Company F is an up-and-coming online retailer. Part of their success is a bespoke multi-Cloud native customer management application. Company F cares about cost only and does not want to, even potentially, pay any more the hosting of their solution, for additional legal guarantees. After all, while this is not a given, the legal level limits the amount of services that are considered for the application and may thus unintentionally weed out the cheapest option.	Tier 3 (basic legal safeguards)	Company F self-identifies as requiring minimal guarantees. Hence tier 3 would be the best, so the legal level would in no way potentially be a limiting factor in choosing the cheapest combination of Cloud services.
Company F continuous to grow and thus attracts more media attention and scrutiny. Moreover, a competitor has recently received a data protection fines and company F just finalized its preparation to carry out its initial public offering. On the advice of their legal counsel and DPO, management decides that their customer management application should receive more attention in	Tier 1 (strong legal safeguards)	Given the change in mentality, tier 1 would be advisable, providing maximal guarantees. In a normal situation, perhaps tier 2 would have been the right choice from the start, but all depends on the target user organization's own identified needs.

Scenario	Recommended tier	How the legal level helps
terms of data protection and security, to avoid any scandals.		

2.9.2 Use case: banking

Another use case can be found in the banking sector. In 2017, the European Banking Authority (further: EBA) issued guidelines on outsourcing by banks to Cloud Service providers. [9] This includes any use of Cloud services and is thus relevant for DECIDE. These guidelines, applicable from 1 July 2018 have been restated and interpreted by the national banks. The new integrated guidelines of the EBA on outsourcing arrangements in general, published in February 2019 and applicable from 30 September 2019, fully integrates the 2017 guidelines [10].

Some specific concerns that come from these guidelines are the following:

- Section "Background," paragraph 41 of the 2019 guidelines [10] specifies that security and privacy require special attention, especially in case of CSPs outside the EEA. This is addressed in the legal level through several controls.

- In the same section, paragraphs 42 and further attack the issue of sub-outsourcing and highlight that the conditions of such arrangements should be clear and controlled and that the financial institution/payment institution should always be able to terminate the contract if planned changes in sub-outsourcing should affect the financial institution/payment institution's risk assessment of the use of the CSP's services. Several controls in the legal level also address this.

- Section 13.3 of the 2019 guidelines addressed audit rights and access to information. The principle is that the access and audit possibilities of the supervisory authority must not be limited (paragraph 89) and that financial institutions/payment institutions must use their audit rights (paragraph 90), hence the importance of enough contractual guarantees. Several controls of the legal level already address this.

- Section 13.4 of the 2019 guidelines highlights the importance for the financial institution/payment institution to have adequate options to get out of the Cloud contract. The legal level also addressed this.

Hence, while the 2019 guidelines require additional language to be in the contracts for an institution/payment institution to be compliant, the legal level may nonetheless be used to pre-select CSPs with a high level of protection on the relevant elements (audit, termination rights, security obligations etc.) and hence will require legal level tier 1. Because of the additional compliance burden, which is not reflected in the legal level, the application developer developing for a financial institution/payment institution will have to conclude contracts ad hoc and will not be able to contract through ACSmI.

However, the legal level may be used as a tool to pre-select certain services and providers or to compare certain services and providers which offer contracts that are compliant with the sectoral legislation. Such contract may be concluded outside the DECIDE framework and still be integrated in the multi-Cloud application run through DECIDE, as there is an option to use existing contract and credentials in the DECIDE framework.

In future versions, these additional requirements could become controls and the CSPs could be given the option to upload standard contracts for service provided to financial institutions/payment institutions, although this might not be feasible.

In addition, customized legal level matrixes could be defined on the level of a specific institution or on the sectoral level, including controls for sector-specific contractual elements and sector-specific certificates.

2.9.3 Use case: healthcare

Another interesting use case is the use of Cloud solutions in healthcare.

Healthcare is subject to specific national legislation in the Member States, which might specify conditions for the use of Cloud services, which may be stringent. Let's take electronic health records as an example. A 2014 report on the status of national laws on electronic health records [11] reveals that 15 Member States have additional specific rules on hosting and processing of electronic health records (section 3.3.1 of the Report), some have rules on obtaining a specific prior authorization showing that the security of the systems used is adequate and data protection is guaranteed (section 3.3.2), and some have rules on auditing the system used (section 3.3.4). In those cases, it is logical that the use of a Cloud service for the hosting of such records will mean that the contracts with the CSPs will need to be assessed for, i.e.:

- Security guarantees offered by the CSP
- Data protection guarantees offered by the CSP
- Audit possibilities of the CSP

The legal level touches upon these topics and thus can be useful to ensure that legislation is complied with, by requiring legal level tier 1, which provides maximal guarantees on the security obligations undertaken by the CSP, the audit possibilities (which enables the hospital itself to survive its own audit by the supervisory authority), the several data protection guarantees present in the DPA, etc.

What is clear, in any case, is that healthcare is a sensitive field of application in any case, as the GDPR requires measures to be implemented in proportion to nature of the processing, and healthcare, dealing with health data as a special category of data under Article 9 of the GDPR, will need to apply all GDPR obligations with due extra care.

Hence, even outside any specific national legal obligation, it would be wise for a healthcare institution to use the legal level to guarantee a certain level of legal protection. In most cases, tier 1 would be advisable.

Choosing a legal level tier 1 CSP may not be the only action a healthcare provider needs to take. A risk assessment may be necessary and perhaps additional contractual arrangements are necessary, which would lead to the contracting through ACSmI becoming less useful. In any case however, the legal level can help select the right CSP and service.

Even if national law should require the CSP to be certified or otherwise be registered/authorized in order to be able to offer services in the (public) healthcare, the legal level could still help differentiate between several providers, or to provide an independent assessment of the legal level offered by the provider.

2.9.4 Use case: e-government

A last use case can in general be found in e-government. While the Cloud (and multi-Cloud) obviously has the same benefits as in the private sector, governmental authorities have the added challenge of additional rules and responsibilities in choosing Cloud services.

First, public procurement rules are applicable and may make it difficult to find the right partner. Second, governmental entities, unlike private companies, have duties to uphold against the citizens in general and must thus guarantee a level of protection and security.

To this extent, several governments in the EU have tried to facilitate the procurement of Cloud services and the choice of the right CSP-partner. Examples include the G-Cloud framework in the UK, facilitating the easy procurement of Cloud services that have been deemed to be acceptable through their involvement in a G-cloud call-off contract, and the Belgian G-Cloud program, which is trying to set up a shared governmental hybrid cloud, integrating for a large part public Cloud service offering. As a counterexample, the Spanish approach under the SARA network is based on a model of mostly private Cloud solutions.

Several governments have even tried to go further and to create certification and accreditation mechanisms, either for government only or including for the benefit of the private sector. Examples include the SecNumCloud framework by ANSSI, the national cybersecurity agency of France and C5, the label/framework provided by BSI, the German federal office for information security, or their joint initiative ESCloud, which stand for European Secure Cloud. See on this the aforementioned TECNALIA study published late 2018 on certification schemes for Cloud computing for more information [8].

While the foregoing initiatives may provide guidance, or even limit the choice of CSPs, they do not address the full legal situation offered by the CSP. Certification mechanisms offered by the public sector may be useful, and so may the future cybersecurity certification framework proposed by the cybersecurity act [12], yet it does not address the full legal situation.

Hence, in those circumstances, the legal level may be used to further differentiate between CSPs. Depending on the information processed in the systems at issue (sensitive information, scale of information), and any additional requirements that may apply, tier 2 or tier 1 will likely be more appropriate for governmental services in the Cloud.

Since this is a specific situation, a customized legal level and functionality may need to be programmed into ACSmI in the future to make the legal level functionality easy and accessible for governmental authorities. It could suffice to filter the ACSmI catalogue to pre-approved CSPs (e.g. those with whom there are call-off contracts, those who have obtained a governmental accreditation or approved certification) and then to compare them or select amongst them based on the legal level. This could be done by customizing the legal level and adding specific governmental certifications/accreditations as a simple control. The specifics may depend on the Member State in question, and thus it may be possible that a demand analysis will have to be made as part of the DECIDE exploitation plan to identify which countries should be targeted. Other controls may need to be added to reflect legal aspects (again, potentially country-specific), which are not yet reflected in the general legal level matrix.

In any case, also in government, the legal level can help the target user organization easily translate its complex legal requirements in a simple NFR for a multi-Cloud application, which will pre-select and pre-reject Cloud services that meet or do not meet those requirements.

3. A contractual framework for the legal level

As was explained in D5.3, the legal level needs to have a contractual framework, so that DECIDE users as well as CSPs are correctly informed and take on the necessary obligations for the legal level to function practically speaking (e.g. CSPs have to commit to answering questions relating to a simple control in a binding manner, DECIDE users should acknowledge that the legal level is presented "as is", etc.).

The contractual framework that will need to be put in place is described in what follows in its essential elements. It is at this time not possible to draft the final contracts and add them to this whitepaper since it's is not yet clear whether ACSmI will act as a re-seller or not. However, a first draft of ACSmI's terms and conditions has been delivered.

Please note as well that this is the preferred option, where the CSP is actively engaged with the DECIDE framework and during the onboarding of the Cloud service into ACSmI. If this is not the case, the entity exploiting ACSmI will, when endorsing Cloud services into ACSmI without CSP involvement, take the responsibility upon itself to provide accurate and up-to-date information. Any gaps will be the responsibility of that entity, which is clearly not the preferable route. Ideally, the contractual framework would function as is described in what follows.

The contractual framework consists of the following three documents:

- An assurance policy, detailing toward the DECIDE users (the application developers and target organizations) what aspects are being assessed under the legal level, how legal changes are monitored, how the objectivity and independence of the legal expert is guaranteed, what the logic behind assigning a legal level is, and what responsibilities rest with the client and/or the CSP. It explains that DECIDE takes no responsibility whatsoever for the information being provided by the CSP to be correct.

  Another section of the assurance policy will detail the onboarding process for the CSPs, how the legal level is assigned, how CSPs may interact with the legal expert, provide extra information, update contracts etc. It describes the CSPs obligations, i.a. to notify the entity exploiting ACSmI of changes in contracts or in its situation that affects the simple controls. This section will explain how, in the case of such changes, the re-assessment will be conducted. It also describes what changes in legislation, case law and interpretation, or otherwise in terms of market changes or changes in state of the art will trigger a re-assessment of the service for assigning the appropriate legal level.

- A clause in the contract with the DECIDE users (i.e. the application developers and/or the target user organizations) referring to the assurance policy detailing the aspects of what the legal level provides and what it does not.

- A contract with the CSPs, which must be made binding upon the CSP before onboarding a service, detailing what the CSPs rights and obligations are, e.g. providing truthful information, undertaking the obligation to notify any change of their contracts or their answers to the questions based on the simple controls, their right to protest the assessment of their service etc. This describes the details of the interaction between the CSP and ACSmI and is aimed at limiting responsibility while creating an amicable relationship with the CSPs. This contract will need to address the question of liability and warranties as well, to enable ACSmI to not be burdened by such commercial risk. The contract could also require CSPs to warrant GDPR compliance before being able to be onboarded in ACSmI, as a further supporting aspect to ensure that tier 3 Cloud services are at least compliant in basic terms.

4. Legal awareness component ACSmI and the legal level

The legal awareness component of ACSmI described in the Description of Action of the DECIDE project is simple the technical implementation of the legal level as presented in this whitepaper. It is detailed in the main deliverable D5.4 and will be fully implemented towards the end of the DECIDE project.

This section merely elaborates on the requirements that follow from this white paper that must be implemented into the ACSmI tool and UI.

The following requirements were identified as must haves:

- The legal level as an NFR must be a minimum requirement. In other words, services with a higher tier of the legal level than requested must not be excluded on the basis that they do not strictly meet the set tier.
- Section 2.6 and the procedure described there must be possible in the tool. This includes the following:
    - There must a verification mechanism that the CSP has accepted the contractual terms of ACSmI
    - The CSP must be able to upload the contractual documents and submit additional information or updates on contracts
    - The CSP must be able to answer the questions related to the simple controls.
    - It must be possible for the legal expert to answer control per control, with an open text box for justification. There must be a log kept of this. The totality of the expert's assessment must be able to be made available to the CSP and must be exportable in a common and human readable format.
    - The tool must allow for the procedure to be repeated.
    - The legal expert must be able to assign a legal level. This must also be able to be changed later on.
    - The tool should provide an interaction possibility with the CSP to enable steps 5 to 7 of section 2.6.1
    - There should be an option for the CSP to withdraw the service from ACSmI.
    - During onboarding, some controls are not relevant in all cases, namely those related to data being sent outside the EEA. The possible location of the service must be easily accessible for the legal expert. It must either be possible to skip these controls if not relevant, or there must be a filtering mechanism, which allows the legal expert to include or exclude those controls based on the possible locations for that service. This must also be registered in the log.

5. Sustainability and upscaling

In section 2.3.1 above it was explained why the legal level was constructed in the current way, making a combination of:

- CSP self-declared simple controls; and
- Legal expert-verified layered controls.

Nonetheless, it could be envisioned that in the future, the legal level may be further developed in the future. What changes and developments will be feasible and useful will depend on both internal and external factors. The following outlines a few routes that may at the time of writing be considered for the future functioning and exploitation of the legal level in ACSmI.

A **first** change that could be valuable would be that **certain of the simple controls would also be verified by the legal expert directly.** This could be an added value service for DECIDE for paying members. In part, this will also depend on the evolution of the means by which an external party will be able to ascertain/verify the presence of these controls without being privy to confidential information held by the CSP. To give an example: if a reliable DPO certification would be developed and there would be an independent service for the legal expert to consult whether a CSP's DPO was GDPR-certified, then it would be possible to make this into a control the legal expert could decide on by him/herself. In that case, simple controls could be transferred to the legal expert.

This may be relevant since even on simple controls (present/not present) opinions might differ. For example, if one compares the CCSM procurement tool on ENISA's website [13], with a recent study carried out by TECNALIA on Certification Schemes for Cloud Computing [8], one comes to different conclusions about what certification schemes meets all of the CCSM's 27 security objectives. It is to be expected that CSPs might come to different results also. To avoid any inconsistency, in the future, it could be envisioned that the legal expert will make this determination and thus deal with all CSPs in the same way.

Moreover, some simple controls may need to be differentiated as well. For example, the EU Data Protection Code of Conduct for Cloud Service Providers drafted by the Cloud Select Industry Group [6], if approved under Article 40 GDPR, itself provides three levels of adherence. To take this into account the simple control would need to be differentiated.

In general, it may be necessary **to update and change controls** because of changes in legislation, interpretation, the Cloud market, standards, uptake of certain schemes or changes in state of the art. This may also lead to changes in the general matrix of the legal level.

In addition to updating existing controls and the manner in which they are assessed, it might be necessary in the future to add controls to the matrix. Examples of controls that could be added in the future would be adherence to approved codes of conduct under Article 40 GDPR beyond those already included and potential certifications under Article 42 GDPR. Certification other than under the GDPR (security, information management) could also still play a larger role in the legal level. Adding certain controls on this could be a next step. One example of a scheme around which a control could be centred is the planned European Cybersecurity Certification Scheme proposed under the proposal for the Cybersecurity Act [12]. Such a scheme could be a relevant simple control, although it also provides for three levels of assurance (basic, substantial and high) and thus needs to be diversified before inclusion. As schemes become industry standards or part of the state of the art, they may be added as new controls insofar existing controls do not yet cover them.

The DECIDE alliance will assess if it is feasible and useful to set up its **own certification mechanism** to complement the legal level.

Another option to further improve the legal level would be to offer a service where the client itself can assign weight and importance to the controls and/or add or delete controls **to customize the legal level** to its specific needs. Alternatively, the legal level could be **customized to the sector** in which the DECIDE user is active. A customization service on the user-specific level could also offer the sector-specific version of the legal level as a template. **Customization** may in addition also be possible based on the **country and applicable law** of the DECIDE user. These options are to be explored in the coming months and years.

Last, but not least, it could be envisioned that some of the tasks that currently require the manual input of the legal expert could be automated. As explained in section 2.6 above, the legal level is assigned after manual review of the contractual documents and the answers on the simple controls. Moreover, the continuous monitoring for legal changes (changes in legislation, case law, interpretation) that may arise and may trigger a re-assessment of the legal level is also done by a human legal expert. It has to be considered if either of these aspects could be **automated** through the use of **legal tech, including artificial intelligence**. While this would not replace the legal expert, it could significantly reduce the input required and could also be used to remove any human bias. The log that will be kept in ACSmI can be useful for this.

6. Conclusions

This whitepaper set out the approach taken to the legal level in ACSmI. It shows how the legal level is built and where the potential value lays for application developer, and through the application developer the target user organization, by enabling in one simple step that only Cloud services that meet the identified legal needs will be considered for deployment of the multi-Cloud application.

While meant primarily to illustrate the status quo in the DECIDE project at M30, it also may serve as a starting point for further tool-driven facilitation of legal compliance in complex and dynamic multi-Cloud environments.

References

[1] E. P. a. t. C. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and; on the free movement of such data, and repealing Directive 95/46/EC," Brussels, [online] available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, 2016.

[2] DECIDE Consortium, "D5.3 Intermediate Advanced Cloud Service meta-Intermediator (ACSmI)," November 2018. [Online]. Available: https://decide-h2020.eu/sites/decide.drupal.pulsartecnalia.com/files/documents/D5.3%20Intermediate%20Advanced%20Cloud%20Service%20meta-intermediator_v1.0_20181130.zip. [Accessed May 2019].

[3] ENISA, "Cloud certification schemes metaframework," ENISA, [online], available at https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework, 2014.

[4] E. P. a. t. Council, *Regulation on a framework for the free flow of non-personal data in the European Union,* [Online], availalbe at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1546942605408&uri=CELEX:32018R1807, 2018.

[5] S. I. C. D. Group, "Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud Services," [online], available at http://cloudswitching.eu/wp-content/uploads/2018/06/20180611-Cloud-Portability_CoC_Draft_V016-PublicConsultationR1.docx, 2018.

[6] "EU Data Protection Code of Conduct for Cloud Service Providers," [online], available at https://eucoc.cloud/fileadmin/cloud-coc/files/former-versions/European_Cloud_Code_of_Conduct_2-0.pdf, 2018.

[7] CISPE, "Data Protection Code of Conduct for Cloud Infrastructure Service Providers," [online], available at https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf, 2017.

[8] Tecnalia, "Certification Schemes for Cloud Computing - final report (SMART 2016/0029)," 2018.

[9] European Banking Authority (EBA), *Recommendations on outsourcing to cloud service providers,* [online] available at https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf/e02bef01-3e00-4d81-b549-4981a8fb2f1e, 2017-2018.

[10] European Banking Authority (EBA), *Final Report on EBA Guidelines on outsourcing arrangements,* [online$, available at https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements, 2019.

[11] Milieu Ltd. and Timelex, *Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services,* [online], available at

https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf, 2014.

[12] E. Commission, *Proposals for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency" and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certficiation ("Cybersecurity Act"),* [online], available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN, 2017.

[13] E. C. S. I. G. certfication, "Cloud Certification Schemes Metaframework online procurement tool," [online], available at https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/cloud-certification-schemes-metaframework, 2015.