EUROPEAN
COMMISSION

Brussels, 19.11.2025
C(2025) 7750 final

ANNEX

ANNEX

to the

COMMUNICATION TO THE COMMISSION

Approval of the draft Commission Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts (with Annexes), annexed hereto

DRAFT COMMISSION RECOMMENDATION

on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), and in particular Article 41 thereof,

Whereas:

(1) Fair contractual rights and obligations are conducive to trust between market participants and can support the increase in fair access and use of data as well as a more competitive market for data-processing services, thus realising the full benefits of a data economy in the Union.

(2) In order to respond to the needs of the digital economy and to remove barriers to a well-functioning internal market for data, Regulation (EU) 2023/2854[1] established a harmonised framework specifying who is entitled to use product data or related service data, under what conditions and on what basis. The central tool which Regulation (EU) 2023/2854 uses for this purpose are contracts. Since the application of that Regulation, the use of data are no longer based on a *de facto* control over data, but on contracts. This is done to create legal certainty as regards the rights and obligations of the parties and thus to promote data sharing. In addition, Regulation (EU) 2023/2854 seeks to ensure, through balanced contracts, a fair share of the benefits for all parties in the data value chain.

(3) Regulation (EU) 2023/2854 provides for rights and obligations of parties involved in data access and use, setting rules for mandatory data sharing, while making it possible for the parties to determine through contracts the practical exercise of their rights and obligations in relation to such data access and use.

(4) Data-processing services are a fundamental enabler for the digital transition and a key factor for competitiveness in the digital age. A customer's ability to switch from one service to another, or to use the services of several providers simultaneously, is a key condition for a more competitive market with lower entry barriers for new providers. Regulation (EU) 2023/2854 sets rules concerning the rights of customers to switch away from a data-processing service provider to another provider or to on-premises infrastructure, and provides specific conditions and procedures, which also cover security and business continuity during the switching process. Regulation (EU)

[1] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj.

2023/2854 also accounts for an in-parallel use of multiple data-processing services, supporting a successful deployment of multi-cloud strategies. In addition, Regulation (EU) 2023/2854 provides that all parties involved in switching must cooperate in good faith.

(5) The rights and obligations of customers and providers of data-processing services are defined in data-processing service contracts. Regulation (EU) 2023/2854 introduces an obligation for data-processing service providers to remove obstacles that might inhibit customers from switching, including contractual obstacles.

(6) Pursuant to Article 41 of Regulation (EU) 2023/2854, the Commission is tasked with developing model contractual terms for data access and use and standard contractual clauses for cloud computing contracts, as a tool supporting the parties in negotiating and concluding such contracts and for promoting models that contain fair, reasonable and non-discriminatory contractual rights and obligations.

(7) According to Regulation (EU) 2023/2854, the primary purpose of these models is to help enterprises, in particular SMEs, to draft, negotiate and conclude such contracts. Regulation (EU) 2023/2854 also states that these model contractual terms, when used widely and integrally, should have the beneficial effect of influencing the design of contracts regarding access to and the use of data and therefore lead more broadly towards fairer contractual relations when accessing and sharing data.

(8) These purposes show that model contractual terms and standard contractual clauses should play an important part in the application of Regulation (EU) 2023/2854 and in showing how balanced contracts applying Regulation (EU) 2023/2854 could be designed, including for courts when applying the general clause of the unfairness control laid down in Regulation (EU) 2023/2854. Furthermore, as provided in recital 55 of Regulation (EU) 2023/2854, dispute settlement bodies should take the model contractual terms into account in order to ensure the uniform application of the Regulation.

(9) Contractual freedom is an essential concept in business-to-business relationships and, as such, is covered by the freedom to conduct a business under the Union Charter of Fundamental Rights of the European Union The Commission is hereby providing market participants with models for their contractual relations which are non-binding in nature and, if the contracting parties choose to use them, they can be adapted, as also explained in Annex I, introducing the model terms and clauses. These terms and clauses were primarily developed for business-to-business relationships taking into account Regulation (EU) 2023/2854 and other Union legislation. As is the case for all contracts, when parties engage in contractual relationships related to data, they need to comply with mandatory provisions of Union law, such as Regulation (EU) 2023/2854, Regulation (EU) 2016/679[2] or the mandatory provisions of consumer law, as well as with mandatory provisions of the national law that is applicable to that particular contract.

[2] 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 (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(10) Unfair contractual terms could make access to data or switching data-processing service providers commercially less viable and sometimes economically prohibitive.

(11) Regulation (EU) 2023/2854 introduces an unfairness control of contractual terms on data access and use or liability and remedies for the breach of the termination of data-related obligations, when unilaterally imposed by a party in contracts concluded between enterprises. The model terms and standard clauses also considered the provisions dealing with this unfairness control.

(12) It is necessary to lay down model contractual terms for several contracts that cover data access and use within the scope of Chapters II, III and IV of Regulation (EU) 2023/2854. The first recommended model contract regulates the legal relationship between a user of a connected product or related service, who is entitled under Regulation (EU) 2023/2854 to access and use data, and a data holder (Annex II). While these model contractual terms may be used as a separate contract in parallel with other contracts, namely a) the contract for the purchase, rent or lease of a connected product, b) the contract on the supply of related services or c) any contract that is necessary to conclude under Regulation (EU) 2016/679 they may also be integrated into an overall contract, for instance covering the purchase of the connected product. The second type of contract covered by the model contractual terms is between the user and a data recipient (Annex III). The third model contract covered is between the data holder and a data recipient, concerning cases where a data holder has a legal obligation to make data available to a third party, such as an obligation to make connected product or related services data available to a data recipient indicated by the user (Annex IV). The fourth model contract covered is concluded between enterprises sharing data on a voluntary basis and is subject to the unfairness control under Regulation (EU) 2023/2854 (Annex V).

(13) It is necessary to lay down standard contractual clauses that can be included in data-processing services contracts to reflect the rights and obligations of customers and providers, in light of Chapter VI of Regulation (EU) 2023/2854 and considering the necessity to remove contractual obstacles to switching and to ensure fair, reasonable and non-discriminatory contractual rights and obligations (Annexes VI to XII).

(14) To facilitate the use of the model terms and standard clauses, guidance and explanations in the form of information boxes should be included. The guidance and explanations are meant to support the parties by providing references to the relevant legal obligations, cross-references between the terms and clauses and, whenever necessary, by explaining the consequences of the choices the parties have to make, as reflected in the various options for a given contractual term or clause,

RECOMMENDS:

(1) That contracting parties use the model contractual terms on data access and use as set out in Annexes I to V.

(2) That contracting parties use the standard contractual clauses as set out in Annexes I and VI to XII -for cloud computing contracts.

(3) That Member States promote the use of the recommended model contractual terms and standard contractual clauses, including through their designated dispute settlement bodies and competent authorities provided for in Regulation (EU) 2023/2854.

[…]

Done at Brussels,

For the Commission
[…]
Member of the Commission

ANNEX I: GENERAL INTRODUCTION

1. Background

In 2022, the Commission set up an Expert Group formed by experts appointed in their personal capacity to support the Commission in providing practical tools to the market participants that would be exercising new rights and obligations under Regulation (EU) 2023/2854 (referred to below as Data Act).. The experts drafted model contractual terms (MCTs) for data access and use and standard contractual clauses (SCCs) for data-processing services. These MCTs and SCCs were included in a Report, published in April 2025 on the group's registry . The Expert Group was supported by a sub-group comprising companies and European and national business organisations. The sub-group gave feedback to the experts throughout the drafting process.

In order to provide additional input to the experts, the Commission services organised not only targeted consultations by testing the draft models with companies that volunteered for this exercise, but also two rounds of public consultation (one on the version of the MCTs and SCCs prepared by the experts and one on the finalised versions included in the Report by the Expert Group).

On the basis of the Report by the Expert Group and of the input received during the public consultation events and as required under Article 41 of the Data Act, the Commission prepared the MCTs and SCCs, included as annexes to this Recommendation.

The MCTs and SCCs are nonbinding. They are and have been drafted in such a way that they can be adapted by the parties according to their contractual needs. However, the parties need to consider that these MCTs and SCCs were drafted to be in line with the rights and obligations provided by the Data Act and were also designed to be consistent with each other. They include information about their voluntary nature and advice for the parties to consider regarding the legal consequences when making changes. In addition, dispute settlement bodies designated under Article 10 of the Data Act should take into account the MCTs and the SCCs.

The MCTs and SCCs were drafted mainly for business-to-business contractual relations. However, they can also be used in relations between businesses and consumers. In that case, however, additional provisions would need to be added to bring the contract into compliance with mandatory consumer protection rules (e.g. the right of withdrawal of the consumer in the case of contracts concluded online/at a distance).

Use of these MCTs and SCCs does not absolve the parties from of their obligation to ensuring ensure compliance with any applicable mandatory provisions of Union or national law. The use of the MCTs and SCCs is at the complete discretion of the parties. The Commission is not liable for any consequences stemming from the use of the clauses.

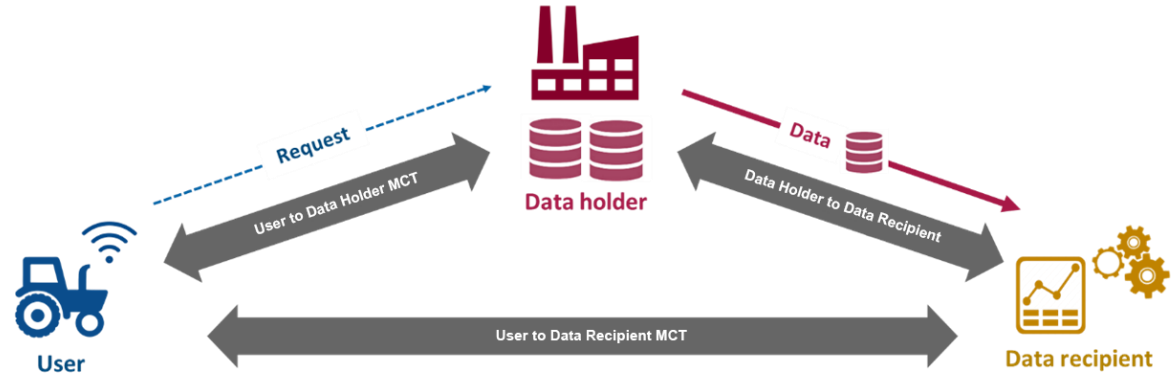
The Commission may review these model contractual terms and standard contractual clauses in light of their application and effect on businesses and market practices.

2. Model contractual terms

The MCTs set out in Annexes II-V have been developed to help parties draft and negotiate contracts for access to and use of data (personal and non-personal). These contracts aim to ensure fair, reasonable and non-discriminatory contractual rights and obligations, including reasonable compensation and the protection of trade secrets.

The contractual parties are defined at the beginning of each of the MCTs, following, where relevant, the terms defined by the Data Act: data, data holder, user, data recipient, etc.

Which MCTs to use for which type of data sharing?



The MCTs in Annex II have been designed for contracts between a data holder and a user of a connected product or related service, where the data holder wishes to use data generated using the product/service.

The MCTs in Annex III have been designed for contracts between a user of a connected product or related service and a third-party data recipient, where the user requests a data holder to make data available to a data recipient under Article 5 of the Data Act.

The MCTs in Annex IV have been designed for contracts between a data holder and a third-party data recipient who is a business, where a data holder is obliged (under Article 5 of the Data Act) to make data available to a recipient when requested to do so by a user of the product. They may also be used with appropriate amendments where a data holder is obliged to make data available to a third-party data recipient under other Union law or national legislation adopted under Union law.

The MCTs in Annex V have been designed for contracts between a data sharer and a data recipient where the data sharer wishes to make data available to a data recipient voluntarily and independent of any request by a user or similar party. The term ‘data sharer’ was chosen to take into account the multiple scenarios that are possible here.

The parties should identify their own situation by reference to the different scenarios explained above and then use the relevant MCTs.

Legal value of the MCTs in relation to the Data Act and other applicable laws

Use of the MCTs by contracting parties does not affect any of the rights and obligations they have under the Data Act or under other Union law or Member State laws adopted in accordance with Union law, including obligations of the controller and the rights of data subjects under Regulation (EU) 2016/679, and under competition law.

The parties should pay particular attention when the sharing of data concerns personal data or mixed datasets. In particular, data holders must make available personal data to users or third parties, as mandated under Regulation (EU) 2023/2854, but only as long as there is a legal basis in accordance with Regulation (EU) 2016/679.

As for any contract, the use of the model contractual terms by the parties does not prevent a competent court or tribunal or any competent administrative authority from setting aside the contract or particular terms thereof for non-compliance with Union law or Member State law.

3. Standard contractual clauses

These SCCs are intended to assist the parties with the contractual implementation of the rights and obligations stemming from the Data Act. The SCCs are a set of modular clauses, which complement each other, but can also be used separately. They are meant to be inserted into Data-Processing Services Agreements.

The SCCs aim to help customers and providers of all Data-Processing Services within the scope of the Data Act, whether public, private or otherwise, small, mid-sized or large.

In line with the Data Act's definition of a Data-Processing Service, these SCCs are applicable to all cloud service models, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), where they display the characteristics laid down in Article 2(8) of the Data Act.

The SCCs under the Data Act do not incorporate the GDPR[3] requirements. Contractual provisions to ensure compliance with the GDPR should be included in the agreement. The Commission has adopted standard contractual clauses for the controller-processor relationship, both to assist with the compliance with the GDPR and for the transfer of personal data to countries outside the EEA[4].

The standard contractual clauses under the GDPR allow entities using them to ensure and demonstrate compliance with certain requirements of the GDPR. Those standard contractual clauses cannot be modified by the parties, they can be included in a broader contract or used as stand-alone agreement.

[3] 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 (General Data Protection Regulation), (OJ L 119, 4.5.2016, pp. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

4 Publications on the Standard Contractual Clauses (SCCs) - European Commission

How to use the SCCs?

While it is recommended to use the whole set of SCCs, it is important to note that these SCCs do not constitute the entire Agreement for Data-Processing Services that would apply between a customer and a provider. Further topics not addressed by the Data Act and the SCCs need to be part of such an Agreement.

A set of 'Definitions' used in the different SCCs and aligned with the Data Act is set out in Annex XII. If definitions other than those proposed in the SCCs are used, the SCCs have to be adapted accordingly. This is just one example of adaptations that are possible while still using the complete set, or a part of the SCCs.

For ease of reference, the SCCs contain cross-references linking certain provisions of the SCCs to relevant provisions in the Data Act or to other SCCs.

There may be additional rules and requirements applicable to Data-Processing Services in specific sectors which should also be considered (for example, in the financial, health, telecom, industry, energy or public sector). The Data Act provides for exceptions to certain obligations related to the SCCs Switching & Exit. Further explanations can be found in the SCCs Switching & Exit.

The Data Act provides for specific possibilities for addressing disputes:

(a) customer and provider have access to a dispute settlement body designated by Member States in accordance with Article 10((4) of the Data Act; and
(b) each of the parties can lodge a complaint with the competent authority in their Member State in accordance with Article 37((5)(b), of the Data Act.

However, at the time of designation, the Member States define the tasks and powers of the competent authority concerned, which may vary to a certain extent between different Member States. It is possible that such an authority is not competent to settle all disputes between the customer and the provider. The parties must assess the most appropriate way to oblige the other party to fulfil its legal and contractual obligations, and how to settle disputes.

The parties may agree to cover multiple services in one single Agreement, which may be called the 'master services agreement' or given another title ('the Agreement'). This is another reason why it is recommended to add the SCCs to the Agreement. If it covers all services, and if the customer decides to switch one or a given number of services, the Agreement will continue to be in force for the other services.

If the parties intend to use these SCCs only partially or to make changes to them, they should carefully consider how this might affect the contractual rights and obligations. Legal and other professional advice is always recommended in such situations.

Model Contractual Terms

ANNEX II: MODEL CONTRACTUAL TERMS
for contracts on data access and use between data holders and users of connected products and related services

These model contractual terms ('MCTs') are meant to address data access and use and related contractual matters that may arise between a Data Holder and users (as defined by Regulation (EU) 2023/2854 – referred hereto as the 'Data Act').

The main novelty of the Data Act in this respect is that:

- users are granted the right to access the data generated by their connected products and/or related services (with protective measures for data protected as trade secrets);
- users can also share that data with third parties, e.g. to benefit from aftermarket services;
- the Data Holder needs to conclude a contract with the user to use and share non-personal data;
- unfair contractual terms concerning access to and use of the data, or liability and remedies for a breach or the termination of data-related obligations, are non-binding if they have been imposed unilaterally on an enterprise by another enterprise.

This Contract has a modular structure, and while it can be used as a full contract, the Parties can also select certain clauses that fit their particular situation. Some terms might not be relevant for all products and all contracts, for example those concerning the protection of trade secrets or the application of technical protection measures. These should be included by the Parties in the contract only where relevant. Similarly, limitations of the access, use or sharing of data would need to be included in the contracts only where relevant, i.e. if the security requirements of the product would otherwise be undermined, resulting in a serious adverse effect on the health, safety or security of natural persons.

Several clauses contain options, and here the Parties should reflect on their specific needs, business relationship and interests to identify the right option that best suits their contract.

Some clauses are also marked *(if applicable)* and they should be included if certain conditions are met.

While the MCTs are recommended by the Commission, they are non-binding and may always be derogated from by the Parties.

1. Parties and Product/Related Service(s)

1.1 Parties to the Contract

This Contract on the access to and use of data is made

between

(insert name, contact details and further references) ('Data Holder')

According to the Data Act, 'data older' means '*a natural or legal person that has the right or obligation, in accordance with the Data Act, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service*'.

In most scenarios, the Data Holder can be the manufacturer of the product or provider of the relevant related service, or another party cooperating with the manufacturer or provider that can retrieve the data from the product or related service.

If more than one party can qualify as a Data Holder, this can be dealt with in different ways, for instance:

(a) each of the Parties concludes its own agreement with the User as an independent Data Holder; or

(b) one of the Parties concludes an agreement with the User and therefore acts as the Data Holder; in the absence of an agreement with the User, the other Parties are considered to be third parties within the meaning of clause 3.2. Based on the Contract with the User and on Contracts with these third parties, the Data Holder can coordinate data access and use.

Which of the two possibilities is preferred in a given case depends on many factors. Parties may wish to consider, for example, whether Users prefer to have just one contracting partner and one Contract. Parties should be aware that there is a close link between the choice between the two options and the way Parties phrase clause 3.2.1.

and

[OPTION 1] [*(insert name, contact details and further references)* ('User')]

[OPTION 2] [any Party that identifies itself as the user within the meaning of the Data Act and declares its assent to the terms of this Contract by taking the following steps: *(insert technical steps to be taken by any party qualifying as User, such as information to be provided and confirmations to be made via a user interface)* ('User')]

referred to in this Contract collectively as 'the Parties' and individually as 'the Party'.

According to the Data Act, 'U, 'ser' means '*a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services'*. This Contract may become relevant in a broad range of different scenarios. On one side of the spectrum, we find scenarios where the User is known to the Data Holder and where lawyers on each side negotiate a bespoke contract on data access and use (e.g. an airline buying planes from an airplane manufacturer). On the other side, we find scenarios where mass products and services are rolled out to millions of consumers who are not individually known (and whose identity we may not even wish to be disclosed for data protection reasons) and where individual negotiations are simply impossible (e.g. connected coffee machines).

For scenarios of the latter kind, and many other scenarios in between the extremes, it may be helpful to identify the User not by name but by steps taken (such as creating a user account or simply plugging in a connected coffee machine and agreeing to the terms and conditions provided by clicking 'OK' on a display). Parties should be aware that, in particular in cases where consumers are involved, courts will assess whether the procedure is designed in a way that complies with the rules of applicable general contract law and consumer law, according to which terms and conditions may have to be included in the contract.

1.2 Product/Related Service(s)

This Contract is made with regard to:

(a) the following connected product(s) ('(the Product'): *(insert name and further specifications of the specific connected product or type of products covered by this contract)*;

(b) the following related service(s) ('(the Related Service(s)'): *(insert name and further specifications of the specific related services or type of related services covered by this contract, if applicable)*.

1.2.1 The User declares that they are either the owner of the Product or contractually entitled to use the Product under a rent, lease or similar contract and/or to receive the Related Service(s) under a service contract.

[OPTION 1] [The User commits to provide upon duly substantiated request to the Data Holder any relevant documentation to support these declarations, where necessary.]

[OPTION 2] [Documentation supporting these declarations as well as details as to who is to be considered as the User under this Contract are set out in **Appendix 9**.]

Under the Data Act, the Data Holder must not require a natural or legal person to provide any information beyond what is necessary for the purpose of verifying whether a person qualifies as a User for the purposes of the Data Act. In many situations, in particular for mass consumer goods or business equipment with relatively low sensitivity of the data that is generated (e.g. connected coffee machines, see above), it will normally be disproportionate to make further inquiries.

2. Data covered by the Contract

The data covered by this Contract consists of any readily available Product Data or Related Service(s) Data within the meaning of the Data Act, and includes both non-personal and personal data ('(the Data').

The Data Holder lists the Data in **Appendix 1**, with a description of the type or nature, estimated volume, collection frequency, storage location and duration of retention of the Data.

If, during this Contract, Data other than those specified in Appendix 1 must be made available to the User, **Appendix 1** will be amended accordingly.

According to the Data Act, '**Product Data**' means '*data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, a data holder or a third party, including, where relevant, the manufacturer*'.

'**Related Services Data**' means '*data representing the digitisation of user's actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider*'.

The Product and Related Services Data can be both personal and non-personal data. They include '*data in raw form*' as well as '*data which have been pre-processed for the purpose of making them understandable and useable prior to subsequent processing*'. But they exclude '*information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data*' (Recital (15)).

'**Readily Available Data**' covers '*product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation*'.

As explained in the recitals, this definition excludes '*data generated by the use of a connected product where the design of the connected product does not provide for such data being stored or transmitted outside the component in which they are generated or the connected product as a whole'* (Recital (20)). '*Manufacturer's design choices, and, where relevant, Union or national law that addresses sector-specific needs and objectives or relevant decisions of competent authorities, should determine which data a connected product is capable of making available*.' (Recital (14)).

3. Data use and sharing by the Data Holder

3.1 Agreed use of non-personal Data by the Data Holder

3.1.1 Without prejudice to any legal right to use the Data, the Data Holder undertakes to use the Data that are non-personal Data only for the purposes agreed with the User as follows:

(a) performing an agreement with the User or activities related to such agreement (e.g. issuing invoices, generating and providing reports or analysis, financial projections, impact assessments, calculating staff benefits);

(b) providing support, warranty, guarantee or similar activities or assessing Users', Data Holders' or third parties' claims (e.g. regarding malfunctions of the Product) related to the Product or Related Service;

(c) monitoring and maintaining the functioning, safety and security of the Product or Related Service and ensuring quality control;

(d) improving the functioning of any Product or Related Service offered by the Data Holder;

(e) developing new products or services by the Data Holder, by third parties acting on behalf of the Data Holder (i.e. where the Data Holder decides which tasks will be entrusted to such Parties and benefits therefrom), in collaboration with other parties or through special purpose companies (such as joint ventures);

(f) aggregating these Data with other data or creating derived data, for any lawful purpose, including with the aim of selling or otherwise making available such aggregated or derived data to third parties, provided such data do not allow specific data transmitted to the Data Holder from the connected product to be identified or allow a third party to derive those data from the dataset.

The Parties should set out the purposes for which and all the details of how the Data Holder may use non-personal Data. The list captures the main common uses but the Parties are free to choose from the ones listed in this clause or to add to it.

In agreeing on data use, the Parties may group the Data into categories, if appropriate. Broader categories may include the following:

- **product or service status data** (e.g. configuration, version, diagnostic messages, consumption data, maintenance data);

- **customer usage data** (e.g. activity times, activity types, geolocation of product) – note that these data may in certain cases constitute personal data and will not be covered by this clause but by clause 3.3. and other provisions of the contract;
- **user environment data** (e.g. soil conditions, area size);
- **general environment data** (e.g. weather data).

Parties should be aware that the default wording given above in this set of terms assumes that the purposes listed therein are the purposes pursued by the Data Holder who is a Party to this Contract. For example, when it comes to the development of new products or services, it is assumed that the development activities are pursued by the Data Holder, albeit possibly together with other Parties, such as a component manufacturer. Sharing of Data with such Parties should therefore be allowed by default, as provided for in clause 3.2.1 (a) (i) and (ii).

The use of the Data for independent purposes by third parties would require either that those third parties enter into a separate contract with the User or that the optional clause 3.2.1 (a) (iii) allowing the Data Holder to sell or donate Data with such third parties for their own purposes applies.

The User should assess the consequences of such uses by the Data Holder or third parties for their operations and their interests, especially whether they should be remunerated by the Data Holder, for instance when the Data Holder may sell the Data generated by the User to third parties.

3.1.2 The Data Holder undertakes not to use the Data:

(a) to derive insights about the economic situation, assets and production methods of the User, or about the use of the Product or Related Service by the User in any other manner that could undermine the commercial position of the User on the markets in which the User is active;

[OPTION] [(b) *(specify data uses that, for example, are significantly detrimental to the legitimate interests of the User)]*.

Parties may wish to provide more details of what kind of Data use they consider to be so detrimental that it must be excluded. This will depend on the relevant sector and other circumstances. In particular, the user may wish to exclude:

- the use of particular categories of highly sensitive Data; and/or
- the use of the Data for particular purposes.

None of the Data uses agreed to under clause 3.1.1 may be in contradiction with this clause, and the Data Holder undertakes to ensure, by appropriate contractual, organisational and technical means, that no third party, within the Data Holder's organisation, engages in such Data use.

3.2 Sharing of non-personal Data with third parties and use of processing services

3.2.1 Without prejudice to legal requirements pursuant to Union or national law for a Data Holder to make data available, the Data Holder may share with third parties the Data that are non-personal Data, if:

(a) the Data are used by the third party exclusively for the following purposes:

i) assisting the Data Holder in achieving the purposes permitted under clause 3.1.1;

ii) achieving, in collaboration with the Data Holder or through special purpose companies, the purposes permitted under clause 3.1.1;

iii) [OPTION] [(*specify the purposes the third parties can pursue for their own needs, independently from the Data Holder, and whether the Data are shared for these purposes against compensation or for free*);] and

(b) the Data Holder contractually binds the third party:

i) not to use the Data for any purposes or in any way going beyond the use that is permissible in accordance with the preceding clause 3.2.1 (a);

ii) to comply with the content of clause 3.1.2;

iii) to apply the protection measures required under clause 3.4.1; and

iv) [OPTION 1] [not to share these Data further unless the User grants general or specific agreement for such further transfer. The Data Holder must oblige the third party with whom they share Data to include the clauses corresponding to points (i) to (iv) in their contracts with recipients.] [OPTION 2] [not to share these Data further except as set forth in **Appendix 5**.]

[OPTION] [Further details, including with regard to identity or categories of third parties with whom Data may be shared, restrictions on use of the Data by third parties, as well as further conditions and protective measures, are set out in detail in **Appendix 5**.]

3.2.2 Notwithstanding clause 3.2.1, the Data Holder may use processing services, e.g. cloud computing services (including infrastructure as a service, platform as a service and software as a service), hosting services, or similar services to achieve, for their own account and under their own responsibility, the agreed purposes under clause 3.1.1. The third parties may also use such services to achieve, for their own account and under their own responsibility, the agreed purposes under clause 3.2.1 (a).

3.3 Use and sharing of personal Data by the Data Holder

3.3.1 The Data Holder may use, share with third parties or otherwise process any Data that is personal Data, only if there is a legal basis provided for and under the conditions permitted under Regulation (EU) 2016/679 of the European Parliament and of the Council [5] (GDPR)and, where relevant, Directive 2002/58/EC (Directive on privacy and electronic communications).

3.4 Protection measures taken by the Data Holder

3.4.1 The Data Holder undertakes to apply the protection measures to prevent Data loss and unauthorised access to the Data [OPTION 1] [that are reasonable and appropriate in the circumstances, considering the state of science and technology, potential harm suffered by the

[5] 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 (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

User and the costs associated with the protective measures.] [OPTION 2] [that are set out in detail in Appendix 6.]

Parties should consider whether they wish to include, if needed in a separate Appendix, all the details of how important interests of the User can be effectively protected. Measures may be both of a technical nature (e.g. encryption, firewalls, split storage) and of an organisational nature (e.g. involvement of a trusted third party). As the measures need to be proportionate, their content will vary widely, depending on the nature of the Data and the interests at stake.

4. (if applicable) Data access by the User upon request

These clauses 4 apply if the User cannot access directly the Data from the Product or Related Service in accordance with Article 3 of the Data Act. In that case, the User is entitled to obtain access to the Data from the Holder upon request, in accordance with Article 4 of the Data Act. If the User wants to give access to the Data to a Data Recipient, clauses 7 below apply.

4.1 Obligation to make Data available

4.1.1 The Data, together with the relevant metadata necessary to interpret and use those Data, must be made accessible to the User by the Data Holder, at the request of the User or a party acting on their behalf. The request can be communicated through (*describe procedure for a simple request through electronic means where technically feasible*). For the purpose of verifying that the request is made by the User, the Data Holder shall not require any information beyond what is necessary. *(if applicable)* [If the request is made by a Party acting on behalf of the User, evidence of their mandate is attached to the request.]

Appendix 2 illustrates the details a request may contain.

4.1.2 When the User is not the data subject, the Data Holder shall make the Data which is personal Data only available to the User, when there is a valid legal basis for making personal Data available under Article 6 of Regulation (EU) 2016/679 and only, where relevant, the conditions set out in Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC (Directive on privacy and electronic communications) are met.

In that respect, when the User is not the data subject, the User must indicate to the Data Holder, in each request presented under the previous clause, the legal basis for processing under Article 6 of Regulation (EU) 2016/679 (and, where relevant, the applicable derogation under Article 9

of that Regulation and Article 5(3) of Directive 2002/58/EC) upon which the making available of personal Data is requested.

4.2 Data characteristics and access arrangements

4.2.1 The Data Holder must make the Data available to the User, free of charge for the User, with the Data being of at least the same quality as when it becomes available to the Data Holder, and in any case in a comprehensive, structured, commonly used and machine-readable format.

> 'Metadata' means a structured description of the content or the use of Data facilitating the finding or use of those Data. According to Article 4(1) of the Data Act the metadata must be made available with the Data, to the extent that the metadata is '*necessary to interpret and use'* the Data.
>
> Though the relevant metadata needed to interpret and use those Data are not laid down and must therefore be identified on a case-by-case basis, the Data Act specifies that '*the data to be made available should include the relevant metadata, including its basic context and timestamp, to make the data useable, combined with other data, such as data sorted and classified with other data points relating to them, or re-formatted into a commonly used format'* (Recital (15)).

The Data Holder and User may use the services of a third party (including a third party providing Data Intermediation Services as defined in Article 2 of Regulation (EU) 2022/868 of the European Parliament and of the Council[6]) to allow the exercise of the User's rights under clause 4.1 of this Contract. Such third party will not be considered a Data Recipient under the Data Act and such services may be offered by a provider considered to be a gatekeeper under Article 3 of Regulation (EU) 2022/1925, unless they process the Data for their own business purposes.

> A third party which provides a service on behalf of the Data Holder or User will not be considered a Data Recipient under the Data Act and these services may be offered by a provider considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council[7], unless they process the Data for their own business purposes.

[6] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

[7] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj).

4.2.2 The User must receive access to the requested Data:

(a) easily and securely;

(b) without undue delay;

(if applicable) [(c) continuously and in real time].

4.2.3 In order to meet the requirements of clauses 4.2.1 and 4.2.2, the Data Holder specifies these access arrangements in **Appendix 1**.

Under Article 4(1) of the Data Act, the Data must be made available without undue delay and, where relevant and technically feasible, continuously and in real time.

As there are various ways to implement these legal requirements, the Data Holder should specify all the details of how access is to be provided in Appendix 1. Conditions for access must not undermine any of the rights afforded to the User under the Data Act or other applicable law.

Bearing in mind this restriction, the Data Holder should, as a first step, decide whether they want to provide for:

- full transfer of the Data, i.e. a copy of the Data is transferred to a medium within the User's control:
- by way of transmission triggered by the Data Holder (push), such as online transmission, uploading into the User's cloud space or delivery of a tangible medium on which the Data are stored; or
- by way of retrieval triggered by the User (pull), such as on being provided with an API, access to the Data Holder's cloud space or similar tools that enable the User to access and extract the Data; or
- access to the Data where they are stored, i.e. the Data are accessed and processed on a medium within the control of the Data Holder or a trusted third party, such as by the User logging into a dedicated space on the Data Holder's or trusted third party's servers, but the Data are not transferred to a medium within the User's control, unless special arrangements are made.

Full transfer gives the User maximum liberty, while access to where the data are stored increases risks for Users that their business ideas become known. In addition, under Article 13(5), point(e), of the Data Act, 'a contractual term shall be presumed to be unfair if its object or effect is to (…) prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data provided or generated by that party during the period of the contract or within a reasonable period after the termination thereof'. Therefore, full transfer should be the default rule.

However, full transfer significantly reduces the Data Holder's ability to prevent abuse and to protect their interests, e.g. trade secrets. Therefore, access to and processing of where the Data are stored should also be possible. To reconcile such access with the interests of the User, access to where the data are stored on a medium controlled by a trusted third party will often be preferable over access on a medium controlled by the Data Holder. Access to where the Data are stored should normally still mean remote access, and on-site access should be restricted to extreme situations with the highest degree of sensitivity.

If access is given to where the Data are stored, there are a number of details to solve, including how to make sure that the User's business ideas are not disclosed and which Data the User is allowed to extract and transfer to a medium within their own control (e.g. derived or inferred data resulting from the User's processing activities).

According to Article 4(1) of the Data Act, the Data must be made available without undue delay and, where relevant and technically feasible, continuously and in real time. Therefore, the Data Holder should specify in the appendix whether access can be provided continuously and in real time, and if not, at what frequency.

The Data Holder should also consider a range of further issues, such as what access credentials are required, and which and how many employees of the User may access the Data.

4.2.4 The Data Holder must provide to the User, at no additional cost, the information necessary for accessing the Data in accordance with Article 4 of the Data Act.

This includes, in particular, the provision of information readily available to the Data Holder regarding any rights which third parties might have with regard to the Data, such as rights of data subjects arising under Regulation (EU) 2016/679, or facts that may give rise to such rights.

The Data Holder specifies this information in **Appendix 1**.

The Parties remain free to agree on any additional support, going beyond the requirements of the Data Act, free of charge or for a fee.

4.2.5 The Data Holder undertakes not to keep any information on the User's access to the requested data beyond what is necessary for:

(a) the sound execution of (i) the User's access request and (ii) this Contract;

(b) the security and maintenance of the data infrastructure;

(c) compliance with legal obligations on the Data Holder to keep such information.

4.3 Feedback loops

If the User identifies an incident related to clause 2 on the Data covered by the Contract, to the requirements of clauses 4.2.1 or 4.2.2 or of **Appendix 1** on the Data characteristics and access arrangements and if the User provides the Data Holder with a detailed description of the incident, the Data Holder and the User must cooperate in good faith to identify the reason for the incident.

If the incident was caused by a failure of the Data Holder to comply with their obligations, they must remedy the breach without undue delay. If the Data Holder does not do so, it is considered to be a fundamental non-performance and the User may invoke clause 12 of this Contract). If the User considers their access right under Article 4 (1) of the Data Act to be infringed, the User is also entitled to lodge a complaint with the competent authority, designated in accordance with Article 37(5)(b) of the Data Act.

This clause gives the Data Holder an opportunity to rectify any breach of their legal or contractual obligations. If the Data Holder fails to do so without undue delay, it allows the user to use the

contractual remedies provided for by the Contract in the case of fundamental non-performance of the Contract.

If the User considers their access right under Article 4(1) of the Data Act to be infringed, the User is also entitled to lodge a complaint with the competent authority, designated in accordance with Article 37(5), point (b), of the Data Act. However, the user should be aware that the precise tasks and powers of the competent authorities designated in accordance with Article 37 may vary among Member States.

The User always has the right to seek an effective remedy before the competent court or to refer the dispute to any alternative dispute resolution body.

The User must therefore carefully assess what is the most appropriate way of obliging the Data Holder to comply with their legal and contractual obligations.

4.4 Unilateral changes by the Data Holder

The Data Holder may unilaterally change the specifications of the Data characteristics or the access arrangements stated in **Appendix 1**, if this is objectively justified by the normal conduct of business of the Data Holder, for example by a technical modification due to an immediate security vulnerability in the line of the products or related services or a change in the Data Holder's infrastructure. Any change must meet the requirements of clauses 4.2.1 and 4.2.2.

The Data Holder must give notice of the change to the User at least *(indicate a reasonable period of time)* before the change takes effect.

A shorter notice period may suffice:

(a) where the change does not negatively affect Data access and use by the user; or

(b) where such notice would be impossible or unreasonable in the circumstances, such as where immediate changes are required because of a security vulnerability that has just been detected.

5. (if the Data made available by the Data Holder upon request of the User must be protected as trade secrets) Protection of trade secrets

1. **Trade secrets sharing** – Data Holders cannot, in principle, refuse a Data access request under the Data Act solely on the basis that certain Data are considered to be protected as a trade secret, as this would subvert the intended effects of the Data Act.

   See clauses 5.1.

   Trade secrets – However, if the Data Holder identifies that certain Data covered by this Contract are protected as trade secrets, as defined by Directive (EU) 2016/943[8] (referred to as the 'Trade Secrets Directive'), they are entitled to certain rights, primarily to continue to preserve the confidentiality of the secrets in question.

   Under Article 2(1) of the Trade Secret Directive, the term 'Trade Secret' means information which meets three requirements: (a) it is secret in the sense that it is not, as a body or in the

[8] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; and (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

A 'Trade Secret Holder' means any natural or legal person lawfully controlling such a Trade Secret.

Data can only be identified as trade secrets if they are protected as such by the Data Holder or the Trade Secret Holder when a data access request is made in accordance with Article 4 of the Data Act.

See clause 5.1.1.

2. **Initial identification of trade secrets** – The Data Holders' rights in respect of trade secrets are – initially – only applicable if and to the extent the Data protected as trade secrets is identified in the Contract.

   See clause 5.1.2.

3. **During the Contract** – The Data Holders' rights in respect of trade secrets could, however, also apply during the Contract, regarding new Data to be made available.

   See clause 5.1.3.

4. **Audit rights** – In order to preserve the confidentiality of the Data protected as trade secrets, while not interfering with each others' activities, certain audit rights by means of involving independent third parties may be considered, including mechanisms in the case of disagreements related to the results of the audit report. The Parties may use alternative measures to audits.

   See clause 5.2.3.

5. **Trade Secret Holder rights (1/4)** – The Data Holder (or third-party Trade Secret Holder) may agree with the User on requirements to preserve the confidentiality of the trade secrets as a condition for sharing those identified trade secrets, such as taking certain proportionate technical and organisational measures.

   See clauses 5.2 and 5.3.

6. **Trade Secret Holder rights (2/4)** – If the initial measures do not suffice, the Trade Secret Holder may, on a case-by-case basis, for specific and identified Data protected as trade secrets, either unilaterally increase the level of the measures, or request that additional measures are agreed with the User. If there is no agreement on the necessary measures, the Data Holder may suspend the sharing of specific Data protected as trade secrets, under the conditions set out in the Data Act.

   See clause 5.4.1.

7. **Trade Secret Holder rights (3/4)** – The trade secret holder may also, on a case-by-case basis, refuse to share specific, identified trade secrets, solely in exceptional circumstances and under the conditions set out in the Data Act.

   See clause 5.4.2.

8. **Trade Secret Holder rights (4/4)** – The Trade Secret Holder may withhold or suspend data sharing if the User breaches their obligations related to the protection of trade secrets.

   See clause 5.4.3.

9. **Retention of Data containing Identified Trade Secrets** – If the Data Holder withholds or suspends data sharing in accordance with clauses 5.4.1, 5.4.2 or 5.4.3, the Data Holder will still be obliged to keep the related Data containing Identified Trade Secrets readily available by retaining them until such time as they can be shared within scope of the Contract.

   See clause 5.6.

10. **Third-party identified Trade Secret Holder** – If the Trade Secret Holder is a third party, the Data Holder must make sure that clause 5 also protects their trade secrets and obtain all relevant authorisations by said third party Trade Secret Holder.

    See clause 5.1.2.

5.1 Applicability of trade secret arrangements

5.1.1 The protective measures agreed on in clauses 5.2. and 5.3 of this Contract, as well as the related rights agreed in clause 5.4, apply exclusively to Data or metadata included in the Data to be made available by the Data Holder to the User, which are protected as trade secrets (as defined in the Trade Secrets Directive, held by the Data Holder or another Trade Secret Holder (as defined in that Directive).

5.1.2 The Data identification of data protected as trade secrets and the identity of the Trade Secret Holder(s) are set out in Appendix 4.

The Data Holder declares to the User that they have all relevant rights from any third-party trade secrets holder to enter into this Contract regarding the Data protected as trade secrets.

In accordance with Article 4(6) of the Data Act, ‘, *the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata*’.

Therefore, the Data Holder should identify the Data protected as trade secrets in **Appendix 4**. However, the Data Holder should not be obliged to describe the trade secret itself. It is sufficient to identify the Data which must be protected to ensure the confidentiality of the trade secret, if the analysis of such Data could reveal the trade secret.

5.1.3 If, during this Contract, new data are made available to the User that are protected as trade secrets as set forth in clause 5.1.1, at the request of the Data Holder, Appendix 4 will be amended accordingly.

Until **Appendix 4** has been amended and agreed between the Parties, the Data Holder may withhold or temporarily suspend the sharing of the new data protected as trade secrets. In such case, the decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay. The data holder shall also notify the competent authority designated pursuant to Article 37 of Regulation (EU) 2023/2854 that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented.

5.1.4 The obligations set out in clauses 5.2 and 5.3 remain in effect after any termination of the Contract, unless otherwise agreed by the Parties.

5.2 Protective measures taken by the User

5.2.1 The User must apply the protective measures set out in **Appendix 4** (hereinafter: 'User's Protection Measures').

> Parties should, in a separate appendix, set out all the details of these measures, including for situations when the User shares the data with third parties. Measures may be both technical (e.g. encryption, firewalls, split storage, etc.) and organisational (e.g. internal governance, appropriate identity management and access checks, involvement of a trusted third party, confidentiality agreements).
>
> As the measures need to be proportionate, their content will vary, depending on the nature of applicable trade secret(s). The measures will also depend on whether (i) access is to be provided to where the Data are stored or (ii) the Data are to be fully transferred to the user. In the former case, the Data Holder has a higher degree of control and can apply part of the protective measures themselves, whereas the User may have a lower level of use for the Data. In any case, both Parties will need to focus on achieving the intended effects of the Data Act. For this reason, the various interests need to be balanced while not subverting those intended effects.

5.2.2 If the User is permitted to make the Data available to a third party, the User can share Data protected as trade secrets, if:

(a) they (i) inform the Data Holder, without undue delay, of the fact that Data protected as trade secrets will be made available to a third party; (ii) specify the Data in question and (iii) give the Data Holder the identity, place of establishment and contact details of the third party;

(b) the third party applies the protective measures set out in Appendix 4.

5.2.3 [OPTION] [In order to verify if and to what extent the User has implemented and is maintaining the User's Protection Measures, the User agrees to either (i) annually obtain, at the User's expense, a security conformity assessment audit report from an independent third party chosen by the User; or to (ii) annually allow, at the Data Holder's expense, a security conformity assessment audit from an independent third party chosen by the Data Holder, subject to such independent third party having signed a confidentiality agreement as provided by the User. Such security audit report must demonstrate the User's compliance with clauses 5 and Appendix 4 as applicable at that time. The results of the audit reports will be submitted to both Parties without undue delay.

The User may choose between (i) and (ii). If a Party deems the security audit report obtained at the other Party's expense to be incorrect, they retain the right to obtain a security audit report from another independent third party at their own expense. If this right is exercised, both

independent third-party auditors, together with the Parties, will discuss any difference between those two reports and aim to resolve any pending matters while observing good faith.]

This clause is marked as an option, because the Parties may agree other measures in order to verify the User's compliance with their obligations to implement and maintain the User's Protection Measures.

5.3 Protective measures taken by the Trade Secret Holder

5.3.1 The Data Holder may apply the measures agreed in **Appendix 4** to preserve the confidentiality of the Data protected as trade secrets (hereinafter: 'Data Holder's Protection Measures').

5.3.2 The Data Holder may unilaterally implement appropriate technical and organisational protection solutions, such as a software update, if they do not negatively affect the User under this Contract.

5.3.3 The User undertakes not to alter or remove the Data Holder's protection measures nor the measures taken in accordance with clause 5.3.2, unless otherwise agreed by the Parties.

5.4 Obligation to share and right to refuse, withhold or terminate

5.4.1 Where the Identified User's Protection Measures and the Data Holder's Protection Measures do not materially suffice to adequately protect a particular piece of Data protected as a trade secret, the Data Holder may, by giving notice to the User with a detailed description of the inadequacy of the measures request that additional protection measures be agreed; if there is no agreement on the necessary additional measures after a reasonable period of time and if the need for such measures is duly substantiated, e.g. in a security audit report, the Data Holder may withhold or suspend the sharing of the specific Data in question; in such case, the Data Holder must give notice to the User; the notice must be duly substantiated, indicate which measures have not been agreed, where relevant, the trade secrets concerned, and be given in writing without undue delay; the Data Holder must continue to share any Data protected as trade secrets other than these specific Data.

5.4.2 If, in exceptional circumstances, the Data Holder is highly likely to suffer serious economic damage from disclosure of particular Data protected as a trade secret to the User despite the User's Protection Measures and the Data Holder's Protection Measures having been implemented, the Data Holder may refuse to share or suspend sharing of the specific Data in question.

The Data Holder must give duly substantiated notice without undue delay to the User and to the competent authority designated pursuant to Article 37 of the Data Act.

However, the Data Holder must continue to share any Data protected as trade secrets other than these specific Data.

Refusal or discontinuation of data sharing under Article 4 of Regulation (EU) 2023/2854 is limited to exceptional circumstances. Therefore, the notice must be duly substantiated. Aspects to be taken into account can be, for example, the lack of enforceability of trade secrets' protection in non-EU countries,

the nature and level of confidentiality of the trade secret in question or the uniqueness and novelty of the relevant connected product.

5.4.3 If the User fails to implement and maintain their User's Protection Measures and if this failure is duly substantiated by the Data Holder, e.g. in a security audit report, the Data Holder is entitled to withhold or suspend the sharing of the specific Identified Trade Secrets until the User has resolved the incident.

In this case, the Data Holder must, without undue delay, give duly substantiated notice in writing to the User and to the competent authority designated pursuant to Article 37 of the Data Act.

5.4.4 Clause 5.4.1 does not entitle the Data Holder to terminate this Contract.

Clauses 5.4.2 or 5.4.3 entitle the Data Holder to terminate this Contract only with regard to the specific Identified Trade Secrets, and if:

(a) all the conditions of clause 5.4.2 or clause 5.4.3 have been met;

(b) no resolution has been found by the Parties after a reasonable period of time, despite an attempt to find an amicable solution, including after intervention by the competent authority designated under Article 37 of the Data Act; and

(c) the User has not been awarded by a competent court with a court decision obliging the Data Holder to make the Data available and there is no pending court proceedings for such a decision.

5.5 End of production and destruction of infringing goods

Without prejudice to other remedies available to the Data Holder in accordance with this Contract or applicable law, if the User alters or removes technical protection measures applied by the Data Holder or does not maintain the technical and organisational measures taken by them in agreement with the Data Holder in accordance with clauses 5.2 and 5.3, the Data Holder may ask the User to:

(a) erase the data made available by the Data Holder or any copies thereof; and/or

(b) end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through the Identified Trade Secrets, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where there is a serious risk that the unlawful use of those data will cause significant harm to the Data Holder or to the Trade Secret Holder or where such a measure would not be disproportionate in light of the interests of the Data Holder or the Trade Secret Holder; and/or

(c) compensate a party suffering from the misuse or disclosure of such unlawfully accessed or used data.

5.6 Retention of Data protected as Identified Trade Secrets

5.6.1 Where the Data Holder exercises the right to refuse, withhold or suspend the sharing of Data with the User in accordance with clauses 5.4.1, 5.4.2 and 5.4.3, they will need to ensure that the Data in question is retained, so that said Data will be made available to the User:

(a) once the appropriate protections are agreed and implemented, or

(b) once a binding decision by a competent authority or court is issued requiring the Data Holder to provide the Data to the User.

The aforementionedThis retention obligation ends where a competent authority or court in a binding decision allows the deletion of such retained Data or where the contract terminates.

5.6.2 The Data Holder will bear the necessary costs for retaining the Data under clause 5.6.1. However, the User will cover such costs to the extent that the withholding or suspension of Data sharing occurs in accordance with clause 5.4.3**.**

6. (if the Data are made available by the Data Holder upon request of the User) Data use by the User

6.1 Permissible use and sharing of Data

6.1.1 The User may use the Data made available by the Data Holder upon their request for any lawful purpose and/or, to the extent that the Data are transferred to or can be retrieved by the User, share the Data freely subject to the limitations in clause 6.2.

6.2 Restrictions on the use and sharing of Data

6.2.1 The User undertakes not to engage in the following:

(a) use the Data to develop a connected product that competes with the Product, nor share the Data with a third party for that purpose;

(b) use such Data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable, the Data Holder;

(c) use coercive means or abuse gaps in the Data Holder's technical infrastructure which is designed to protect the Data in order to obtain access to Data;

(d) share the Data with a third party considered to be a gatekeeper under Article 3 of Regulation (EU) 2022/1925.

6.2.2 [OPTION] [Furthermore and in accordance with Article 4(2) of the Data Act, the User and the Data Holder agree to restrict or prohibit as follows the following processing (*specify concerned processing: access, use and/or further sharing of Data*), having as a consequence the undermining of the security requirements for the Product, as laid down by Union law (*specify*

legal security requirement concerned), resulting in a serious effect on the health, safety or security of natural persons.

The User undertakes not to (specify relevant restrictions or prohibitions related to the above-mentioned processing).]

7. Data sharing upon the User's request with a Data Recipient

7.1 Making Data available to a Data Recipient

7.1.1 The Data, together with the relevant metadata necessary to interpret and use those Data, must be made available to a Data Recipient by the Data Holder, free of charge for the User, upon request presented by the User or a party acting on their behalf. The request can be made using the form specified in **Appendix 3**, sent to (*describe procedure for a simple request through electronic means where technically feasible*). For the purpose of verifying that the request is made by the User, the Data Holder shall not be required to provide any information beyond what is necessary.

7.1.2 When the User is not the data subject, the Data Holder shall make the Data which is personal data only available to a third party following a request by the User, when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (GDPR) and only when, where relevant, the conditions set out in Article 9 of that Regulation and in Article 5(3) of Directive 2002/58/EC (Directive on privacy and electronic communications) are met.

In that respect, when the User is not the data subject, the User must indicate to the Data Holder, in each request presented under the previous clause, the legal basis for processing under Article 6 of Regulation (EU) 2016/679 (and, where relevant, the applicable derogation under Article 9 of that Regulation and Article 5(3) of Directive 2002/58/EC) upon which the making available of personal data is requested.

7.1.3 The Data Holder must make the Data available to a Data Recipient, with the Data having at least the same quality as they did when they became available to the Data Holder, and in any case in a comprehensive, structured, commonly used and machine-readable format, easily and securely.

7.1.4 Where the User submits such a request, the Data Holder will agree with the Data Recipient the arrangements for making the Data available in accordance with Chapters III and IV of the Data Act.

7.1.5 The User acknowledges that a request under clause 7.1.1 cannot benefit a third party considered to be a gatekeeper under Article 3 of Regulation (EU) 2022/1925 [OPTION] [and cannot be made in the context of the testing of new connected products, substances or processes that are not yet placed on the market].

7.1.6 The User acknowledges that the third party shall only process the Data made available to them pursuant to clause 7.1.1 for the purposes and under the conditions agreed with the User. The Data Holder may not be held liable towards the User for the absence of such an agreement

between the User and the third party, unless the Data Holder knew or should have known about this absence.

8. [OPTION if the User is a business entity] Limitations on User's rights

The user agrees to (specify the purpose, nature and duration of the limitation of the User's right to use or share the Data and identify the part of the Data concerned by such limitations).

In accordance with Article 7(2) of the Data Act, '*Any contractual term which, to the detriment of the user, excludes the application of, derogates from or varies the effect of the user's rights under [Chapter II] shall not be binding on the user*'.

This should be read in light of Recital (25) which specifies that it '*does not prevent users, in the case of business-to business relations, from making data available to third parties or data holders under any lawful contractual term, including by agreeing to limit or restrict further sharing of such data, or from being compensated proportionately, for example in exchange for waiving their right to use or share such data'.*

Therefore such limitations will only be valid if they do not cause any detriment to the User, meaning that the limitations should not harm the User's legitimate interests.

In addition, this clause should not be used to entirely deprive the User of their legal rights under Articles 4 and 5 of the Data Act, for example by the User completely giving up their right to access Data. The User could only agree to limitations on their rights, when these are limited in scope and time. These, and are not to the User's detriment. This could, for example, be specific limitations on the use of the Data which has been accessed, or involve agreeing not to share the Data further with a third party as indicated in Recital 25, or to not let a Data Recipient further share the Data with a third party.

This clause could be used when the User has an interest in such limitations, for example, when the Data Holder and the User engage in a joint industrial project.

It could also apply if the User is compensated. But the mere receipt of compensation would not be sufficient in itself to consider that limitations are not detrimental to the User. This compensation should be proportionate to the limitations.

The User may at their sole discretion accept or refuse the limitation(s) under this clause.

9. Compensation to the User

9.1 Compensation

The Data Holder undertakes to compensate the User as set out in detail in **Appendix 7**, *(if applicable)* including for the limitations of User's rights in accordance with clause 8.

The Parties can agree on compensation for the Data Holder's use and sharing of the Data, whenever they think it is fair and reasonable. For instance, they may consider such compensation if the Data Holder uses the Data for developing new products or services or if the Data Holder creates aggregated or derived data for commercial purposes. Conversely, if for instance the Data are used exclusively for the needs of any agreement concluded with the User or for ensuring the functioning, safety and security of the Product or Related Service, compensation might not be included.

However, the Parties should be aware that, for example, if the User limits their rights in accordance with clause 8, the User should be compensated, as explained in the explanatory box under clause 8, and the compensation should be proportionate to the gravity of the limitation.

Similarly, compensation might be needed to ensure the fair treatment of the User, if the User agrees that the Data Holder may sell the Data to third parties in accordance with clause 3.2.1 (a) (iii).

If compensation is due, the Parties must agree on its nature, which can be monetary or not.

9.2 (applicable for monetary compensation) Interests in case of late payments

If payment of compensation is delayed, the Data Holder should pay to the User interest on overdue compensation from the time when payment is due to the time of payment as laid down in the applicable law.

10. Transfer of use and multiple users

The Initial User may permanently transfer ownership of the Product or their right to use the Product to a Subsequent User, for example when the user sells the Product (transfer of use).

The Initial User may also grant rights to use the Product and/or receive related services to Additional Users, while still retaining its role as a User (multiple users), for example when:

- a business sublets its van to another business for certain periods of the year;
- a car rental company rents its cars to customers.

Right of the Data Holder to use the Data

In such cases, the Data Holder must conclude a contract with the Subsequent or Additional Users to be able to use data generated by the use of the Product or Related Services by such users. The clauses below propose possible solutions for the conclusion of such a contract, so that the Parties can choose the solution that is most adapted to the specificities of the situation.

In the case of transfer, the Parties could for example agree that the Initial User notifies the Data Holder of the transfer, the identity and the contact details of the Subsequent User so that the Data Holder is able to contact the Subsequent User and conclude a contract with them.

In the case of multiple users, such a solution might be too burdensome for the Data Holder. If the Initial User is in a position to act on behalf of the Data Holder, one possibility is therefore that the Initial User obtains the agreement of Additional Users with the conditions for data access and use set out in this Contract.

In other situations, it may still be feasible and preferrable for the Initial User to notify the Data Holder of the contact details of an Additional User, in such a manner that the Data Holder can conclude a contract directly with the Additional User.

It is also possible that the Data Holder does not need to be notified of a Subsequent or Additional User by the Initial User in order to conclude a contract, because the circumstances are such that they can conclude a contract without any action from the Initial User. For instance, it may happen that the creation of an account identifying the user is required for using the Product and/or Related Service. If this is the case, the Data Holder will be in a position to conclude a contract with the Subsequent or the Additional User when they create their own accounts. However, this could require the Initial User to ensure that the Subsequent or Additional User does not use their account.

Access rights of the Parties in relation to a transfer of use and multiple users

In the case of transfer of use or multiple users, the Contract should give certainty as to who can access the Data and under what conditions. For example, where a company (the Initial User) rents out connected agricultural machinery to individual farmers (Additional Users) on a daily or weekly basis, the data generated by the agricultural machines may disclose sensitive business information of the individual farmers. The manufacturer (the Data Holder) cannot simply make any data under clause 4 of this Contract accessible to the Initial User (the company that owns the machines) without making sure that, by doing so, no confidential information or rights of individual farmers (the Additional Users) are infringed.

Access rights of the Additional or Subsequent User may in particular depend on a contractual categorisation of the Data, for instance:

- User's Removable Data – The products or related services often allow the user to delete the Data generated in the course of their use. In the case of transfer, the user should delete such Data. Otherwise, such Data may be accessible to the Additional or Subsequent User.
- Always Removable Data – Data which the Data Holder should not make accessible to the Additional or Subsequent User.
- Residual Data –Data other than the User's Removable or Always Removable Data; such Data will not be removable and will not be subject to a confidentiality agreement (i.e. the Data will also be available to new Subsequent Users). Such Data may include the Data which needs to be accessible to the Additional or Subsequent User by operation of law or in practice (for example, related to the updates made in a connected vehicle).

The Data Holder should sort the Data into these categories, particularly in the information referred to in Article 3(2) and (3) of the Data Act, in this Contract (for instance, in Appendix 1) or in the documentation relating to the Product or Related Service.

This clause 10 focuses on the Data Act; it does not affect any additional legislation, including sectoral legislation, that could regulate the transfer of a connected product or related service (e.g. reprocessing of medical devices).

10.1 Transfer of use

Where the User contractually transfers (i) ownership of the Product, or (ii) their temporary rights to use the Product, and/or (iii) their rights to receive Related Services to a subsequent person

('Subsequent User') and loses the status of a user after the transfer, the Parties undertake to comply with the requirements set out in this clause.

[OPTION 1] The Initial User must notify the Data Holder of the transfer, and provide the necessary contact details of the Subsequent User, so that the Data Holder can conclude a contract with them regarding the Data Holder's use of the Data.

[OPTION 2] The Data Holder takes the necessary steps to conclude a Contract with the Subsequent User regarding the Data Holder's use of the Data. *(if applicable)* The Initial User must ensure that the Subsequent User cannot use the Initial User's account.

The rights of the Data Holder to use Product Data or Related Services Data generated prior to the transfer will not be affected by a transfer, i.e. the rights and obligations relating to the Data transferred under the Contract before the transfer will continue after the transfer.

10.2 Multiple users

Where the Initial User grants a right to use the Product and/or Related Service(s) to another party ('Additional User') while retaining their status as a User, the Parties undertake to comply with the requirements set out in this clause.

10.2.1 The Additional User's agreement to the use and sharing of Data by the Data Holder

[OPTION 1] In the Contract between the Initial User and the Additional User, the Initial User includes, on behalf of the Data Holder, clauses substantially reflecting the content of this Contract between the Initial User and the Data Holder and in particular clause 3 on the use and sharing of the Product and/or Related Service Data by the Data Holder, for the duration of the temporary use of the Product and/or Related Service.

[OPTION 2] The Initial User notifies the Data Holder of the existence and duration of the Additional User's rights to use the Product and/or Related Service and their contact details, so that the Data Holder can conclude an agreement with the Additional User on the use and sharing of that Data by the Data Holder.

[OPTION 3] The Data Holder takes the necessary steps to conclude an agreement with the Additional User. *(if applicable)* The Initial User must ensure that the Additional User cannot use the Initial User's account.

10.2.2 Data Access by the Additional User

[OPTION] [The Initial User acts as a first contact point for the Additional User, if the Additional User makes a Data access request under Articles 4 or 5 of the Data Act. The Data Holder must collaborate with the Initial User to address the request, as specified in **Appendix 10**.]

10.3 Liability of the Initial User

To the extent that the Initial User's failure to comply with their obligations under clauses 10.1 and 10.2 leads to the use and sharing of Product or Related Services Data by the Data Holder in the absence of a Contract with the Subsequent or Additional User, the Initial User will indemnify the Data Holder in respect of any claims for damages by the Subsequent or Additional User

towards the Data Holder for their use of the Data after the transfer or temporary use of the Product and/or Related Service(s).

11. Date of application, duration of the Contract and termination

11.1 Date of application and duration

This Contract would usually not exist as a standalone contract, but would be concluded in parallel with the contract transferring ownership of the Product to the User, giving them temporary rights to use the Product and/or with the contract for a Related Service.

This Contract must generally remain into force as long as this other contract allows the User to use the Product or Related Service. Similarly, neither the Data Holder nor the User should be able to terminate this Contract except where there is a substantive breach of obligations by the other Party, as this would otherwise result in a situation in which the User uses the Product and/or Related Service without any contractual framework regarding rights and obligations under the Data Act.

11.1.1 This Contract [OPTION 1] [takes immediate effect] [OPTION 2] [takes effect from (*specify date*)].

11.1.2 The Contract is concluded for [OPTION 1] [an indeterminate period] [OPTION 2] [a fixed term of (*specify*)], subject to any grounds for expiry or termination under this Contract.

11.2 Termination

Irrespective of the contract period agreed under clause 11.1, this contract terminates:

(a) upon the destruction of the Product or permanent discontinuation of the Related Service, or when the Product or Related Service loses its capacity to generate the Data in an irreversible manner; or

(b) upon the User losing ownership of the Product or when the User's rights with regard to the Product under a rental, lease or similar agreement or the user's rights with regard to the related service come to an end; or

(c) when both Parties so agree.

Points (b) and (c) shall be without prejudice to the contract remaining in force between the Data Holder and any Subsequent or Additional User.

11.3 Effects of expiry and termination

11.3.1 Expiry of the contract period or termination of this Contract releases both Parties from their obligation to effect and to receive future performance but does not affect the rights and liabilities that have accrued up to the time of termination.

Expiry or termination does not affect any provision in this contract which is to operate even after the contract has come to an end, in particular clause 13.1 on confidentiality, clause 13.4 on applicable law and clause 13.6 on dispute settlement.

11.3.2 The termination or expiry of the Contract will have the following effects:

a) the Data Holder shall cease to retrieve the Data generated or recorded as of the date of termination or expiry;

b) the Data Holder remains entitled to use and share the Data generated or recorded before the date of termination or expiry as specified in this Contract.

12. Remedies for breach of contract

Parties may wish to agree not only on the data-specific rights and obligations (many of which follow already from the Data Act) but also on matters of general contract law, such as the rights and remedies of a contracting party where there is non-performance on the part of the other contracting party.

For such matters of general contract law, Parties may wish to rely on statutory default rules, or on other contract templates. If they wish to use these model contractual terms they should make sure these are compatible with any mandatory national law that may be applicable to the Contract.

12.1 Cases of non-performance

12.1.1 A non-performance of an obligation by a Party is fundamental to this contract if:

(a) the non-performance substantially deprives the other Party of what it was entitled to expect under this Contract, unless the non-performing Party did not foresee and could not reasonably have foreseen that result; or

(b) it is clear from the circumstances that the non-performing Party's future performance cannot be relied on.

12.1.2 A Party's non-performance is excused if it is due to an impediment beyond its control and that that Party could not reasonably have been expected to take the impediment into account at the time of the conclusion of this Contract, or to have avoided or overcome the impediment or its consequences.

Where the impediment is only temporary the excuse has effect for the period during which the impediment exists. However, if the delay amounts to a fundamental non-performance, the other Party may treat it as such.

The non-performing Party must ensure that notice of the impediment and of its effect on its ability to perform is received by the other Party without undue delay after the non-performing

Party knew or could be reasonably expected to have become aware of these circumstances. The other Party is entitled to damages for economic damage resulting from the non-receipt of such notice.

12.2 Remedies

12.2.1 In the case of a non-performance by a Party, the other Party shall have the remedies listed in the following clauses, without prejudice to any remedies available under applicable law.

12.2.2 Remedies which are not incompatible may be cumulated.

12.2.3 A Party may not resort to a remedy to the extent that they cause the other Party's non-performance, such as where a shortcoming in its own data infrastructure did not allow the other Party to duly perform its obligations. A Party may also not rely on a claim for damages suffered to the extent that it could have reduced the damage by taking reasonable steps.

12.2.4 The aggrieved Party can:

(a) request that the non-performing Party comply, without undue delay, with its obligations under this Contract, unless it would be unlawful or impossible or specific performance would cause the non-performing Party costs which are disproportionate to the benefit the other Party would obtain;

(b) request that the non-performing Party erases Data accessed or used in violation of this contract and any copies thereof;

(c) claim damages for economic damage caused to them by the other Party's non-performance which is not excused under clause 12.1.2. The non-performing Party is liable only for damage which it foresaw or could be reasonably expected to have foreseen at the time of conclusion of this contract as a result of its non-performance, unless the non-performance was intentional or grossly negligent.

12.2.5 The Data Holder can also suspend the sharing of Data with the User until the User complies with their obligations or restrictions, by giving a duly substantiated notice to the User without undue delay:

(a) if the non-performance of User's obligations is fundamental;

(b) *(if applicable)* provided that all other conditions set out in clause 5.4.3 are met, in cases described in clause 5.4.3.

12.2.6 The User can also:

(a) suspend the agreement given to the Data Holder under clause 3 or their agreement to the limitations on User's rights agreed under clause 8, until the Data Holder complies with their

obligations, unless this would cause a detriment to the Data Holder that is grossly disproportionate compared to the non-performance or its effects;

(b) withdraw the permission given to the Data Holder under clause 3 and/or their agreement to the limitations on User's rights agreed under clause 8, by giving notice to the Data Holder, if:

(i) the Data Holder's non-performance is fundamental; or

(ii) in the case of non-performance which is not fundamental, the User has given a notice fixing a reasonable period of time to remedy the non-performance and the period has lapsed without the Data Holder performing. The period stated is taken to be reasonable, if the Data Holder does not object to it without undue delay.

12.2.7 [OPTION] [Where a Party fails to perform its obligations under this Contract it shall, in any case, pay the penalties set out in detail in Appendix 8, which the Parties deem damages within the meaning of clause 12.2.4 (c). The non-performing Party has the right to request that the penalty is reduced to a reasonable amount where it can prove that the penalty is grossly excessive in relation to the damage resulting from the non-performance.]

> The Parties may wish to define penalties for defined types of non-performance as it may be too onerous for the aggrieved Party to prove the amount of actual damage caused by, e.g., a failure to supply Data. Penalties should be proportionate.

13. General Provision

13.1 Confidentiality

13.1.1 The following information will be considered as confidential:

(a) information referring to the trade secrets, financial situation or any other aspect of the operations of a party, unless that Party has made this information public;

(b) information referring to the User and any third party, unless they have already made this information public.

13.1.2 Both Parties agree to take all reasonable measures to store securely confidential information and not to make such information available to any third party, unless

(a) one of the Parties is under a legal obligation to or make available the relevant information,

(b) it is necessary for one of the Parties to make the relevant information available in order to fulfil their obligations under this contract, or

(c) one of the Parties has obtained the prior consent of the other Party or the party providing the confidential information or affected by its disclosure.

13.1.3 These confidentiality obligations remain applicable after the termination of the Contract for a period of (*specify the period*).

13.1.4 These confidentiality obligations do not remove any more stringent obligations under (i) the Regulation (EU) 2016/679 (GDPR), (ii) the provisions implementing Directive 2002/58/EC or Directive (EU) 2016/943, or (iii) any other Union law or Member State law (iv) (if applicable) clause 6 of this Contract.

13.2 Means of communication

Any notification or other communication required by this Contract must be in writing and may be delivered by hand, sent by prepaid post, or transmitted by electronic means, including email, provided that the sender retains proof of sending to the addresses listed below:

Party	**Contact Person**	**Email**	**Phone**	**Address**
User	[Name]/[Position]	[Email]	[Phone]	[Address]
Data Recipient	[Name]/[Position	[Email]	[Phone]	[Address]

Any such notice or communication will be deemed to have been received:

(a) if delivered by hand, on the date of delivery;
(b) if sent by prepaid post, on the third business day after posting;
(c) if sent by electronic means, on the date of transmission, provided that no error message indicating failure to deliver has been received by the sender.

13.3 Entire Contract, modifications and severability

13.3.1 This Contract (together with its appendixes and any other documents referred to in this Contract) constitutes the entire Contract between the Parties with respect to the subject matter of this Contract and supersedes all prior contracts or agreements and understandings of the Parties, oral and written, with respect to the subject matter of this Contract.

13.3.2 Any modification of this Contract shall be valid only if agreed to in writing, including in any electronic form.

13.3.3 If any provision of this Contract is found to be void, invalid, voidable or unenforceable for whatever reason, and if this provision is severable from the remaining terms of the contract,

these remaining provisions will continue to be valid and enforceable. Any resulting gaps or ambiguities in this Contract shall be dealt with according to clause 13.5.

13.4 Applicable law

This Contract is governed by the law of *(specify state)*.

13.5 Interpretation

13.5.1 This Contract is concluded by the Parties against the background of the Parties' rights and obligations under the Data Act. Any provision in this Contract must be interpreted so as to comply with the Data Act and other Union law or national legislation adopted in accordance with Union law as well as any applicable national law that is compatible with Union law and cannot be derogated from by agreement.

13.5.2 If any gap or ambiguity in this contract cannot be resolved in the way referred to by clause 13.5.1, this contract must be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 13.4).

13.6 Dispute settlement

13.6.1 The Parties agree to use their best efforts to resolve disputes amicably and, before bringing a case before a court or tribunal, to submit their dispute to (*insert name and contact details of a particular dispute settlement body; for disputes within their competences as defined in Article 10 (1) of the Data Act, it may be any dispute settlement body in a Member State that fulfils the conditions of Article 10 of the Data Act*).

13.6.2 Submission of a dispute to a dispute settlement body in accordance with clause 13.6.1. does, however, not affect the right of the User to lodge a complaint with the national competent authority designated in accordance with Article 37 of the Data Act, or the right of any Party to seek an effective remedy before a court or tribunal in a Member State.

13.6.3 [OPTION, if the user is a business] [The courts of (*specify state*) will have exclusive jurisdiction to hear the case concerning this Contract.]

Appendix 1: Details of the data covered by this Contract and of access arrangements

In this Appendix, the Parties should give the details of the data covered by this Contract, of access arrangements and of the means and information necessary to access and use the data, as stipulated in clauses 2 and 3.

A. Specification of the content of the data

The appendix should first sort and list the Product Data and Related Service Data covered by the Contract, with the indication of the content of the Data and of the collection frequency, so that the User is informed in a precise manner about the information contained in the Data (structured list of data points or precise categories of data).

B. Duration of retention

The appendix should then indicate the duration of retention, so that the User is informed about the duration of the availability of the Data. They may do so in a granular manner for each data points or group of data points.

C. Data regime

The appendix should specify here whether all or part of the Data is particular data regulated by a specific regime. The appendix could e.g. indicate whether and what Data qualifies as personal data.

D. Data structure and format

The appendix should specify here in what structured, commonly used and machine-readable format the Data is made available.

E. Access policy

It may happen that the User transfers their rights to use the Product or to receive the Related Services to a Subsequent User or that multiple users share these rights. In such cases, the parties should specify here the access rights to the Data in case of transfer of use of the product or in case of multiple users. The appendix could in particular list

- User's Removable Data – the products or related services often allow the user to delete the Data generated in the course of their use. In the case of transfer, the user should delete such Data. Otherwise, such Data may be accessible to the subsequent user;
- Always Removable Data – Data which the Data Holder should not make accessible to the subsequent user;
- Residual Data – other Data than User's Removable or Always Removable Data; such Data will not be removable and will not be subject to a confidentiality agreement (i.e. the Data

will also be available to new Subsequent Users). Such Data may include the Data which needs to be accessible to the Subsequent User by operation of law or in practice (for example, related to the updates made in the connected vehicle

F. Transfer/Access Medium

The appendix should indicate here via which secure-convenient electronic medium the Data can be made available by Data Holder to the User, either by transfer or access.

G. Information necessary for the exercise of the User's access rights

The appendix can specify here the information that are necessary for the exercise of the User's access rights. It may include a contact person to solve technical issues, in the Data Holder's side as well as in the User's side.

Appendix 2: Content of an access request by the User

This form is for one particular request. Multiple requests are possible under and are recommended for instance to segment certain data flows so those can be managed from data flow to data flow and from purpose to purpose, data life cycle to data life cycle (such as, for instance personal data flows and the like).

While this form lists key elements of a request, its form may be adapted, in particular to fit with electronic procedures.

Identification of the User	Name: *Specify* Contract n°: *Specify*
Identification of the person making the request on behalf of the User (if applicable)	Name: *Specify* Relationship with the User: *Specify* Please attach evidence of the power to act on behalf of the User
Products and/or Services concerned by the request	Product/Service 1: *Specify (e.g. serial number)* Product/Service 2: *Specify (e.g. serial number)*
Data points concerned by the request	☐ All data which is readily available to the Data Holder ☐ Other: *Specify the data points covered by the request*
Nature of the requested Data	☐ Including personal Data *If the User is not the data subject, specify valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, how the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled* ☐ Only non-personal Data
Date of Data concerned by the request	☐ Past data: *Specify the period* ☐ Future data: *Specify the period*

Timing of access to the Data *(depending on what is specified in Appendix 1)*	☐ Continuously ☐ Realtime ☐ Other: *please specify*
Modalities for access to the Data *(depending on what is specified in Appendix 1)*	☐ Transfer of the Data ☐ Access to the Data where it is stored
Destination for the transfer:	*Specify depending on the answer to the previous point*
Date of the request	*Specify*

Appendix 3: Form for an access request by the User to make data available to a third party

This form is for one particular request. Multiple requests are possible under and are recommended for instance to segment certain data flows so those can be managed by a particular Data Recipient as appointed by User from data flow to data flow and from purpose to purpose.

Identification of the User	Name: *Specify* Contract n°: *Specify*
Identification of the person making the request on behalf of the User (if applicable)	Name: *Specify* Relationship with the User: *Specify*
Products and/or Services concerned by the request	Product/Service 1: *Specify* Product/Service 2: *Specify*
Data concerned by the request 3.4.2 **Please note:** does not apply in the context of the testing of new connected products, substances or processes that are not yet placed on the market	☐ Option 1: All data which is readily available to the Data Holder ☐ Option 2: *Specify, in accordance with Appendix 1 of the contract between the User and the Data Recipient specifying the Data to be shared with the Data Recipient* ☐ Option 3: As specified by the Data Recipient in appendix 2 of the contract between the Data Holder and the Data Recipient
If the data includes personal data	*Specify valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, how the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled*
Identification of the third party	Name: *Specify* Contact details: *Specify*

3.4.3	**Please note:** cannot be a gatekeeper under Article 3 of Regulation (EU) 2022/1925	

Appendix 4: Details of measures for the protection of trade secrets

(to be drafted by the parties)

[OPTION] Appendix 5: Details on sharing data with third parties

(to be drafted by the parties)

Appendix 6: Details of protection measures

(to be drafted by the parties)

[OPTION] Appendix 7: Details on compensation of the User

(to be drafted by the parties)

[OPTION] Appendix 8: Details on penalties

(to be drafted by the parties)

[OPTION] Appendix 9: Documentation on ownership of the Product or contractual rights to use the Product or Related services

(Documentation to be attached by the parties)

[OPTION] Appendix 10: Details on data access arrangements by Additional Users

(to be drafted by the parties)

ANNEX III: MODEL CONTRACTUAL TERMS
for Contracts between Users and Data Recipients

These model contractual terms have been designed for Contracts between a User of a connected product and/or related service and a Data Recipient with whom the User needs or wishes to share their data under Article 5 of Regulation (EU) 2023/2854 (referred hereto as the 'Data Act').:

The main novelty of the Data Act in this respect is that:

- the User can oblige the Data Holder to share Data with a Data Recipient of their choice;
- the User determines in a Contract with the Data Recipient for what purposes and under what conditions the Data Recipient can use and share data;
- unfair contractual terms concerning access to and use of the Data, or liability and remedies for a breach or the termination of data-related obligations, are non-binding if they have been imposed unilaterally on an enterprise by another enterprise.

This Contract would often follow the contract that is concluded between the data holder and the user, and precede the contract that also needs to be concluded between the Data Holder and the Data Recipient.

This Contract has a modular structure and while it could exist as a stand-alone Contract by using all the clauses (when data sharing is the main purpose of the Contract), the Parties can also select certain clauses that fit their particular situation. If data sharing was only a precondition for the fulfilment of a contract concluded for another purpose, e.g. a contract for repair and maintenance of an industrial machine, it could be sufficient to use clauses 1.2, 1.3, 2, 3 and 4 (except clause 4.1.1(b)), since the content of the remaining clauses in this Contract would likely be covered by the repair and maintenance contract.

1. Parties and Product/Related Services

1.1 Parties to the Contract

This Contract on the access to and use of data is made between

(insert name, contact details and further references) ('User')

and

(insert name, contact details and further references) ('Data Recipient')

referred to in this Contract collectively as 'the Parties' and individually as 'the Party'.

'User' is a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.

'Data Recipient' is a third party of the User's choice. They can be either a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the User of a connected product or related service, to whom the Data Holder makes data available, including a third party following a request by the User to the Data Holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law.

Such a Data Recipient may be in competition with the relevant Data Holder. However, a gatekeeper is not eligible to become or be a Data Recipient.

1.2 Eligibility of the Data Recipient

The Data Recipient declares that they are not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925[9] ('Digital Markets Act').

1.3 Request to the Data Holder and cooperation of the Parties

1.3.1 The Parties agree that

[OPTION 1] the User will request

(*insert name, contact details and further references*) ('Data Holder')

to make the Data specified in clause 2 available to the Data Recipient.

[OPTION 2] the User mandates the Data Recipient to request the

(*insert name, contact details and further references*) ('Data Holder')

on behalf of the User to make the Data specified in clause 2 available to the Data Recipient.

1.3.2 The User and the Data Recipient will cooperate in good faith to arrange for adequate contact and engagement with the Data Holder. In particular, the Data Recipient will enter into a separate contractual agreement with the Data Holder ('H2R Contract'), [OPTION: in close consultation with the User] and in line with applicable law including but not limited to the Data Act. The Data Recipient must ensure that the H2R Contract complies with this Contract.

1.3.3 This Contract is made with regard to:

(a) the following connected product(s) ('the Product'): *(insert name and further specifications of the specific connected Product covered by the Contract)*;

(b) the following related service(s) ('the Related Service(s)'): *(insert name and further specifications of the specific Related Services or type of Related Services covered by the Contract, if applicable)*.

The User declares that they are either the owner of the Product or contractually entitled to use the Product under a rent, lease or similar contract and/or to receive the Related Service(s) under a service contract.

[OPTION 1] The User commits to provide upon duly substantiated request to the Data Recipient any relevant documentation to support this declaration, where necessary.

[OPTION 2] Documentation supporting this declaration as well as details as to who is to be considered the User under this Contract are set out in **Appendix 5.**

[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj)

2. Data covered by the Contract

The Data covered by this Contract consist of all readily available Product Data or Related Service(s) Data generated by the use of the Product or by the Related Services:

[OPTION 1] [within the meaning of the Data Act.]

[OPTION 2] [within the meaning of the Data Act, as listed in Appendix 1.]

[OPTION 3] [within the meaning of the Data Act, as is necessary for purposes agreed under clause 3 and further listed by the Data Recipient in Appendix 2 of the H2R Contract.]

The User is not responsible for quality, characteristics and quantity of the Data and their fitness for a particular purpose.

According to the Data Act, '**product data**' means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a User, a Data Holder or a third party, including, where relevant, the manufacturer.

'**Related services data**' means data representing the digitisation of the User's actions or of events related to the connected product, recorded intentionally by the User or generated as a by-product of the User's actions during the provision of a related service by the provider.

The product and related services data can be both personal and non-personal data.

'**Readily available data**' covers '*product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation*'.

As explained in the recitals, this definition excludes '*data generated by the use of a connected product where the design of the connected product does not provide for such data being stored or transmitted outside the component in which they are generated or the connected product as a whole'* (Recital (20)). '*Manufacturer's design choices, and, where relevant, Union or national law that addresses sector-specific needs and objectives or relevant decisions of competent authorities, should determine which data a connected product is capable of making available*.' (Recital (14)).

3. Data use by the Data Recipient

Data sharing agreements between Users and Data Recipients could, for example, be a new relationship or could be an addition to an existing relationship between the Parties, whether for commercial data-sharing purposes or not. Such agreements should be non-exclusive, except for cases that are well-scoped, data-specific, market-specific, purpose-specific, time-limited and well remunerated.

3.1 Agreed use of the Data

It is up to the User to consider which part of their Data and for what purpose they would allow the Data Recipient to use the Data and in particular to what extent the Data Recipient should be allowed to share the Data with other third parties.

For example, the User may ask the Data Recipient to monitor the functioning of the Product or related service and act as an intermediary notifying warranty claims to the seller of the equipment on behalf of the User.

The User should also consider whether to allow the Recipient to share the Data with commercial or non-commercial entities. Non-commercial data sharing may include altruistic or otherwise not-for-profit sharing and use for public interest, scientific, statistical or other analytical research purposes (where applicable and required, or not applicable or required but envisioned in conformity with Article 89 GDPR, the Open Data Directive (EU) 2019/1024, the High Value Dataset Regulation (EU) 2023/138, the Data Governance Act (EU) 2022/868, the Health Data Spaces Regulation (EU) 2025/327, and the like), by or through the Data Recipient with relevant communities, municipalities, regions, nations, NGOs, and other non-commercial organisations. For commercial data sharing, it is recommended not to refer to or use the term 'sale' as that may imply for some stakeholders that the title/control of the relevant Data is transferred, or that such relevant Data are otherwise handed over to the Data Recipient exclusively. This is neither needed nor recommended, especially since Data are both a digital asset and a digital means, and can be used for many purposes throughout their life cycle – even multiple commercial purposes – while still granting a Data Recipient market advantage or other value creation that also justifies a fair remuneration to the User for granting such licence to (re)use the Data.

The User should assess the consequences of granting the Data Recipient the right to use, and if applicable, share the data and also consider whether such rights should be granted in exchange for compensation.

3.1.1 The Data Recipient may only use the Data for the following purposes, which cannot be in contradiction with the practices listed in clause 3.2: *(insert agreed purposes)*.

Examples of agreed purposes by the Data Recipient:

- offer regular maintenance/aftermarket services of the Product to the User;
- conduct research within specific fields;
- develop new services or improve, upgrade or sustain new products or services, including artificial intelligence (AI) solutions;
- aggregate the Data with other data or create derived data, for any lawful purpose, including with the aim of selling or otherwise making available such aggregated or derived data to third parties.

3.1.2 The Data Recipient must erase the Data when the Data are no longer required for the agreed purposes.

3.2 Non-authorised use of the Data

The Data Recipient may not use the Data:

(a) for any purpose other than the purposes agreed in clause 3.1;

(b) for any purpose that is in violation of Union law or applicable national law;

(c) for the profiling of natural persons within the meaning of Article 4(4) of the GDPR, unless it is necessary to provide the service requested by the user

(d) to develop a product that competes with the Product;

(e) to derive insights about the economic situation, assets and production methods of the User, or about the use of the Product or Related Service by the User in any manner that could undermine the commercial position of the User on the markets in which the User is active, unless the User has given permission for such use;

(f) in a manner that adversely impacts the security of the Product or any Related Service;

(g) [OPTION] [other: *(specify, in particular, uses that are significantly detrimental to the legitimate interests of the User)*].

3.3 Use of personal data by the Data Recipient

The Data Recipient shall use or otherwise process any Data that are personal data only if there is a legal basis provided for this and only under the conditions laid down in Regulation (EU) 2016/679 (GDPR) and, where relevant, Directive 2002/58/EC (Directive on privacy and electronic communications).

In regulating the processing of personal data in accordance with the applicable data-protection legislation (including but not limited to Regulation (EU) 2016/679), the Parties must consider whether the User is the data subject of all or part of the personal data contained in the Data.

3.4 Application of protective measures

The Data Recipient undertakes to apply protection measures to prevent Data loss and unauthorised access to the Data [OPTION 1] [that are reasonable in the circumstances, considering the state of science and technology, potential harm suffered by the User and the costs associated with the protective measures.] [OPTION 2] [as set out in detail in **Appendix 2**.]

Parties should consider whether they wish to include, in a separate Appendix, all the details of how important interests of the User can be effectively protected. Measures may be both of a technical nature (e.g. encryption, firewalls, split storage) and of an organisational nature (e.g. involvement of a trusted third party). As the measures need to be proportionate, their content will vary widely, depending on the nature of the Data and the interests at stake.

4. Data sharing with third parties and use of data-processing services

In accordance with Article 6 (2) (c) of the Data Act, the Data Recipient cannot '*make the data it receives available to another third party, unless the data is made available on the basis of a contract with the user, and provided that the other third party takes all necessary measures agreed between the data holder and the third party to preserve the confidentiality of trade* secrets'.

Therefore, if the User chooses to give the Data Recipient this right, this clause should be inserted, possibly in exchange for compensation.

4.1 Conditions for data sharing

4.1.1 The Data Recipient may share Data which are non-personal data with third parties if:

(a) the Data are used by the third party exclusively for the following purposes:

(i) assisting the Data Recipient in achieving the purposes agreed in clause 3.1;

(ii) achieving, in collaboration with the Data Recipient or through special purpose companies, the purposes agreed in clause 3.1.; and

(iii) [OPTION] [*(please specify the particular purposes the third parties can pursue for their own needs, independently from the Data Recipient, and whether the Data are shared for these purposes in exchange for compensation or for free)*; and]

(b) the third party is not designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925 ('Digital Markets Act'); and

(c) the Data Recipient contractually binds the third party:

(i) not to use the Data for any purposes other than the purposes agreed in clause 4.1.1 (a);

(ii) not to derive insights about the economic situation, assets and production methods of the User, or about the use of the Product or Related Service by the User in any other manner that could undermine the commercial position of the User on the markets in which the User is active;

(iii) not to use Data in a manner that is otherwise significantly detrimental to the legitimate interests of the User, in particular when such data contain commercially sensitive data or are protected by trade secrets or by intellectual property rights;

(iv) to apply the protection measures required under clause 3.4; and

(v) to erase the Data when the Data are no longer necessary for the purposes agreed in clause 4.1.1 (a);

(vi) not to share these Data further.

4.1.2 Further details, including the identity of the third parties, restrictions on use of the data by third parties, as well as further conditions and protective measures, are set out in detail in **Appendix 3**.

4.1.3 Notwithstanding clauses 4.1.1 to 4.1.2, the Data Recipient may use processing services, e.g. cloud computing services (including Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service), hosting services, or similar services to achieve, for their own account and under their own responsibility, the agreed purposes under clause 3.2.1 (a). The third parties may also use such services to achieve the agreed purposes under clause 4.1.1 (a), for their own account and under their own responsibility. The Data Recipient shall share with third parties or otherwise process any Data that are personal data only if there is a legal basis provided for and

under the conditions permitted under Regulation (EU) 2016/679 (GDPR) and, where relevant, Directive 2002/58/EC (Directive on privacy and electronic communications).

5. Compensation

The Data Recipient undertakes to compensate the User as set out in detail in **Appendix 4.**

The Parties can agree on compensation for the Data Recipient's use and sharing of the Data, whenever they think it is fair and reasonable. For instance, they may consider such compensation if the Data Recipient uses the Data for developing new products or services or if the Data Recipient creates aggregated or derived data for commercial purposes. Conversely, if for instance the Data are used exclusively for the needs of any agreement concluded with the User, compensation might not be included.

Similarly, compensation might be needed to ensure the fair treatment of the User, if the User agrees that the Data Recipient may sell the Data to third parties in accordance with clause 4.1.1 (a) (iii). If compensation is due, the Parties must agree on its nature, which can be monetary or not.

6. Date of application, duration of the Contract and termination

6.1 Date of application and duration

6.1.1 This Contract [OPTION 1] [takes immediate effect] [OPTION 2] [takes effect from *(specify date)*].

6.1.2 [OPTION] [This Contract is concluded for [OPTION 1] [an indeterminate period] [OPTION 2] [a fixed period of (specify)], subject to any grounds for expiry or termination under this Contract.]

6.2 Termination

6.2.1 The Data Recipient may terminate this Contract by giving notice within (*specify notice period*) to the User if the H2R Contract has been terminated.

6.2.2 If the User loses their status as a User, this Contract terminates. The User will give notice within (*specify notice period*) to the Data Recipient.

6.2.3 [OPTION in the case of an indeterminate period or if the Parties wish to allow termination for convenience] [Either Party may terminate this Contract at any time before the start of or during the contract period by giving (*specify period*) notice to the other Party.] [OPTION] If the User terminates this Contract under this clause before *(insert point in time or minimum contract period)*, the User shall compensate the other Party for the costs incurred in relation to the implementation of this Contract, as follows: *(specify as appropriate)*.

In cases where the User is contractually obliged to share Data with the Data Recipient, this clause should not be included as it could lead to a breach of another contract.

6.3 Effects of expiry or termination

6.3.1 Expiry of the contract period or termination of this Contract releases both Parties from their obligation to effect and to receive future performance but does not affect the rights and liabilities that have accrued up to the time of expiry or termination.

Expiry or termination does not affect any provision which is to operate even after the Contract has come to an end, in particular any limitations on the permissible use and sharing of the Data by the Data Recipient under clauses 3 and 4, clause 8.1 on confidentiality, clause 8.3 on applicable law and clause 8.6 on dispute resolution.

6.3.2 In particular, the termination or expiry of the Contract will have the following effects:

(a) the Data Recipient shall immediately cease to retrieve the Data generated or recorded as of the date of termination or expiry;

(b) [OPTION] the Data Recipient remains entitled to use and share the Data generated or recorded before the date of termination or expiry as specified in clauses 3 and 4 **[**OPTION for a period of *(specify time)*].

There may be cases where the Data Recipient needs to investment in data sharing, such as by adapting their digital infrastructure; the investment will be amortised over time. In this case, the Parties may want to make sure that the Data Recipient receives compensation from the terminating Party. The amount of the compensation should be determinable.

7. Remedies for non-performance

7.1 Cases of non-performance

7.1.1 A non-performance of an obligation by a Party is fundamental if:

(a) the non-performance substantially deprives the other Party of what they were entitled to expect under this Contract, unless the non-performing Party did not foresee and could not reasonably have foreseen that result; or

(b) it is clear from the circumstances that the non-performing Party's future performance cannot be relied upon.

7.1.2 A Party's non-performance is excused if it is due to an impediment beyond their control and if that Party could not reasonably have been expected to take the impediment into account at the

time of the conclusion of this Contract, or to have avoided or overcome the impediment or its consequences.

7.1.3 Where the impediment is only temporary, the excusing of the Party's non-performance has effect for the period during which the impediment exists. However, if the delay amounts to a fundamental non-performance, the other Party may treat it as such.

The non-performing Party must ensure that notice of the impediment and of its effect on their ability to perform is received by the other Party without undue delay after the non-performing Party knew or could be reasonably expected to have become aware of these circumstances. The other Party is entitled to damages for economic damage resulting from the non-receipt of such notice.

7.2 Remedies for non-performance

7.2.1 In the case of a non-performance by a Party, the other Party shall have the remedies listed in the following clauses, without prejudice to any remedies available under applicable law.

7.2.2 Remedies which are not incompatible may be cumulated.

7.2.3 A Party may not resort to a remedy to the extent that they cause the other Party's non-performance, such as where a shortcoming in their own data infrastructure did not allow the other Party to duly perform their obligations. Nor may a Party rely on a claim for damages suffered to the extent that they could have reduced the damage by taking reasonable steps.

7.2.4 The aggrieved Party can:

(a) terminate this Contract with immediate effect without penalty, by giving notice to the other Party, if:

(i) the other Party's non-performance is a fundamental non-performance; or

(ii) in the case of non-performance which is not fundamental, the aggrieved Party has given notice fixing a reasonable period of time to remedy the non-performance and the period has lapsed without the other Party performing;

(b) claim damages for economic harm caused to them by the other Party's non-performance which is not excused under clause 7.1.2; the non-performing Party is liable only for damage which it foresaw or could be reasonably expected to have foreseen at the time of conclusion of this Contract as a likely result of its non-performance, unless the non-performance was intentional or grossly negligent;

(c) request that the non-performing Party complies, without undue delay, with its obligations under this Contract, unless it would be unlawful or impossible or specific performance would cause the non-performing Party costs which are disproportionate to the benefit that the other Party would obtain; [OPTION] [where a Party fails to perform their obligations under this Contract they shall, in any case, pay the penalties set out in detail in **Appendix 6**, which the Parties deem damages within the meaning of clause 7.2.4 (b); the non-performing Party has the right to request that the penalty is reduced to a reasonable amount where they can prove that the penalty is grossly excessive in relation to the damage resulting from the non-performance.]

8. General provisions

8.1 Confidentiality

8.1.1 The following information must be considered confidential:

(a) information referring to the trade secrets, financial situation or any other aspect regarding the operations of the other Party unless the other Party has made this information public;

(b) (*if applicable*) information setting out the basis for the calculation of the compensation;

(c) information referring to the Data Holder and any other protected third party, unless the protected third party has made this information public.

8.1.2 Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 8.1.1. and not to disclose or make available such information to any third party, unless:

(a) one of the Parties is under a legal obligation to disclose or make the relevant information available; or

(b) it is necessary for one of the Parties to disclose or make the relevant information available to fulfil their obligations under this Contract; or

(c) one of the Parties has obtained the prior consent from the other Party or the party providing the confidential information or affected by its disclosure.

8.1.3 In any case, the User and the Data Recipient may disclose or make available such information to the Data Holder as is necessary to identify or contact the Data Recipient or the User in order to enter into the H2R Contract as referred to in clause 1.3.2.

8.1.4 These confidentiality obligations remain applicable after the termination of the Contract for a period of (*specify the period*).

8.1.5 These confidentiality obligations do not remove any more stringent obligations under (i) Regulation (EU) 2016/679 (GDPR), (ii) the provisions implementing Directive 2002/58/EC or Directive (EU) 2016/943 or (iii) any other EU or Member State law.

8.2 Means of communication

Any notification or other communication required or permitted to be given under this Contract must be in writing and may be delivered by hand, sent by prepaid post, or transmitted by electronic means, including email, provided that the sender retains proof of sending to the addresses listed below:

Party	Contact Person	Email	Phone	Address
User	[Name]/[Position]	[Email]	[Phone]	[Address]
Data Recipient	[Name]/[Position	[Email]	[Phone]	[Address]

Any such notice or communication will be deemed to have been received:

(a) if delivered by hand, on the date of delivery;
(b) if sent by prepaid post, on the third business day after posting;
(c) if sent by electronic means, on the date of transmission, provided that no error message indicating failure to deliver has been received by the sender.

8.3 Entire Contract, amendments and severability

8.3.1 This Contract (together with its Appendices and any other documents referred to in it) constitutes the entire Contract between the Parties with respect to the subject of this Contract and supersedes all prior agreements or contracts and understandings between the Parties, oral or written, as regards the subject of this Contract.

8.3.2 Any amendment to this Contract will be valid only if agreed to by the Parties in writing, including in any electronic form.

8.3.3 If any provision of this Contract is found to be void, invalid, voidable or unenforceable for whatever reason, and if this provision is severable from the remaining terms of the Contract, these remaining provisions will be unaffected by this and will continue to be valid and enforceable, unless the provision is not severable from the remaining provisions of this Contract. Any resulting gaps or ambiguities in this Contract must be dealt with pursuant to clause 8.4.

8.4 Applicable law

This Contract is governed by the law of *(specify state)*.

8.5 Interpretation

8.5.1 This Contract is concluded by the Parties against the background of the Parties' rights and obligations under the Data Act. Any provision in this Contract must be interpreted so as to comply with the Data Act and other Union law or national legislation adopted in accordance

with Union law, as well as any applicable national law that is compatible with Union law and cannot be derogated from by agreement.

8.5.2 If any gap or ambiguity in this Contract cannot be resolved in the way referred to in clause 8.5.1, this Contract must be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 8.4).

8.6 Dispute settlement

8.6.1 The Parties agree to use their best efforts to dissolve disputes amicably and, before bringing a case before a court or tribunal, to submit their dispute to *(insert name and contact details of a particular dispute settlement body; for disputes within their jurisdiction as defined in Article 10(1) of the Data Act, it may be any dispute settlement body in a Member State that meets the conditions of Article 10 of the Data Act)*.

8.6.2 [OPTION, if the User is a business] [The courts of *(specify state)* will have exclusive jurisdiction to hear the case concerning this Contract.]

Appendix 1 contains a description of the Data

[To be drafted by the Parties]

Appendix 2 lists the protective measures to be taken by the Data Recipient

[To be drafted by the Parties]

Appendix 3 contains information on sharing the Data with third parties by the Data Recipient

[To be drafted by the Parties]

Appendix 4 contains information on compensation to the User for the Data Recipient's use and sharing of the Data

[To be drafted by the Parties]

Appendix 5 contains documentation on ownership of the Product or contractual rights to use the Product or Related services

[To be drafted by the Parties]

[OPTION] Appendix 6 contains details on penalties

[To be drafted by the Parties]

ANNEX IV: MODEL CONTRACTUAL TERMS
for contracts between Data Holders and Data Recipients on making data available at the request of users of connected products and related services

These model contractual terms have been designed for Contracts between a Data Holder and a Data Recipient who is a business, where a Data Holder is obliged (under Article 5 of Regulation (EU) 2023/2854 – referred hereto as the 'Data Act') to make Data from a connected product and/or related service available to a Data Recipient when requested to do so by the User.

The main novelty of the Data Act in this respect is that:

- the Data Holder is obliged to share Data with the Data Holder upon receiving a request from the User to do so (with protective measures for Data protected as trade secrets);
- the Data Holder can ask for reasonable compensation from the Data Recipient;
- unfair contractual terms concerning access to and use of the Data, or liability and remedies for a breach or the termination of data-related obligations, are non-binding if they have been imposed unilaterally on an enterprise by another enterprise.

This Contract has a modular structure, and while it can be used as a full contract, the Parties can also select certain clauses that fit their particular situation. Several clauses contain options, and here the Parties should reflect on their specific needs, business relations and interests to identify the right option that best suits their Contract.

Some clauses are also marked *(if applicable)* and they should be included if certain conditions are met.

While the model contractual terms are recommended by the Commission, they are non-binding and may always be derogated from by the Parties.

These model contractual terms may also be used with appropriate amendments where a Data Holder is obliged to make Data available to a Data Recipient under other Union law or national legislation adopted in accordance with Union law.

1. Parties, Requesting User and Product/Related Service(s)

1.1 Parties to the Contract

This Contract on the access to and use of data is made

between

(insert name, contact details and further references) ('Data Holder')

and

(insert name, contact details and further references) ('Data Recipient')

referred to in this Contract collectively as 'the Parties' and individually as 'the Party'.

The Parties must identify here who is the Data Holder and who is the Data Recipient, within the meaning of Article 2(13) and (14) of the Data Act.

According to the Data Act, data older' means a natural or legal person that has the right or obligation, in accordance with the Data Act, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, Product Data or Related Service Data, which it has retrieved or generated during the provision of a related service.

According to the Data Act, 'data recipient' means a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the User of a connected product or related service, to whom the Data Holder makes Data available, including a third party, following a request by the User to the Data Holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law. In accordance with Article 1(3)(d) of the Data Act, data holders are only obliged to make Data available to '*Data Recipients in the Union*'. They are not obliged to do so to Data Recipients whose place of establishment is outside the Union.

1.2 Requesting User, Product/Related Service(s)

1.2.1 This Contract is based on the joint assumption of the Parties that the Data Holder is obliged under Article 5 of the Data Act to make data available to the Data Recipient when requested to do so by or on behalf of

(insert name, contact details and further references) ('Requesting User')

and that the Requesting User is a User (within the meaning of Article 2(12) of the Data Act) of:

(a) the following Product: (*insert name and further specifications of the specific connected product or type of products covered by the Contract); and/or*

(b) the following Related Service(s): *(insert name and further specifications of the specific related service(s) or type of related service(s) covered by the Contract, if applicable).*

The Parties must identify here who is the User within the meaning of Article 2(12) of the Data Act, that makes a request to the Data Holder, under Article 5 of the Data Act

A 'User' means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.

The Parties must also identify which connected product and, if applicable, which related service is used by the Requesting User.

According to the Data Act, '**connected product**' means an item:

(i) that obtains, generates or collects data concerning its use or environment;

(ii) that is able to communicate product data via an electronic communications service, a physical, connection or on-device access;

(iii) whose primary function is not the storing, processing or transmission of data on behalf of third parties, other than the User.

'**Related service**' means a digital service (other than an electronic communications service, including software) which:

(i) is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions; or

(ii) is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product.

2. Basis of the Contract

2.1 Quality of the Requesting User and existence of a valid request

2.1.1 Each Party declares that, to the best of their knowledge, the Requesting User is a User (within the meaning of Article 2(12) of the Data Act) of the Product and Related Service(s) specified in clause 1.2.1.

2.1.2 Each Party declares that the Requesting User has requested that the Data Holder makes available to the Data Recipient the Data specified in clause 3.1. Evidence of the request is attached to this Contract in **Appendix 1**.

2.1.3 *(If applicable)* Each Party declares that, to the best of their knowledge, the Party acting on behalf of the Requesting User has received the necessary authority from the Requesting User to submit this request in accordance with applicable law. Evidence of the authorisation is attached to this Contract in **Appendix 1**.

Under the Data Act, the request may be made by a third party acting on behalf of the Requesting User. This third party may, for example, be a data broker or any other agent or representative, including the Data Recipient themselves.

Obviously, if a third party, including the Data Recipient, claims to have been authorised by the Requesting User, this situation is a potential source of abuse compared to the usual request situation. Therefore, the Parties must take reasonable steps to verify that there has been no fraud or manipulation and that this request has been correctly submitted.

2.1.4 Each Party declares that, to the best of their knowledge, the request is valid under applicable law, has not been withdrawn and has not expired.

If there are indications that the request is invalid or has been withdrawn, the Parties must take reasonable steps to verify that there is still a request that is valid. If this is not the case, the Data Holder may not be allowed to share the data with the Data Recipient and may be liable for doing so. The Data Recipient may also be liable for requesting data they are not entitled to request.

The validity of the request may depend on many factors under applicable law. For example, for a request to be legally valid, it could be necessary for it to:

- qualify as a freely given, sufficiently informed and explicit indication of the Requesting User's wishes;
- be given with the legal capacity required.

2.2 Eligibility of the Data Recipient

2.2.1 The Data Recipient declares that there is a contract in force between them and the Requesting User allowing them to use the Data and that, according to this contract, the Data will be used exclusively for (*insert purpose(s) according to contract between Data Recipient and Requesting User)*:

(if the Data may disclose trade secrets) The Data Recipient declares that the Data are strictly necessary for fulfilling this purpose.

> In accordance with Article 6(1) of the Data Act, the Data Recipient can only use the Data on the basis of a contract concluded and for the purposes agreed with the User. The Data Recipient should make declarations here confirming that this is the case. If these declarations are not or no longer correct, the Data Holder may have the possibility to terminate the contract in accordance with clause 2.4.3.
>
> The Parties should endeavour to establish the agreed purposes in a way that allows the Data Holder to determine whether the use of the Data by the Data Recipient is permissible, but not so detailed as to reveal to the Data Holder confidential business ideas belonging to the Data Recipient.
>
> Where the Data Holder's trade secrets are at stake, the full purposes must be disclosed, to enable the Data Holder to assess whether the provision of the data is strictly necessary to achieve the stated purpose.

2.2.2 The Data Recipient declares that it is not designated as a 'gatekeeper' pursuant to Article 3 of Regulation (EU) 2022/1925 ('Digital Markets Act').

2.3 Compliance with data-protection law

2.3.1 As far as the Data qualifies as personal data, each Party declares that they comply with Regulation (EU) 2016/679 and, where relevant, Directive 2002/58/EC.

2.3.2 In particular, when the Requesting User is not the data subject, the Data Holder may only make the Data which are personal data available to the Data Recipient, to the extent permitted under Regulation (EU) 2016/679 and, where relevant, Directive 2002/58/EC.

> The concept of 'personal data' under the GDPR is very broad. It covers any data that relate to an identified or identifiable person, i.e. a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
>
> Non-personal data can become personal data, for example when they are part of a mixed dataset, where they are combined with new data and the outcome of this combination makes it possible to link the data to an identified or identifiable individual. This can also happen where new data-processing capabilities emerge.
>
> The Parties should start by carefully assessing the existence of personal data in the Data as well as their own roles, and that of the User, under the GDPR:
>
> - '**data subject**' is the identified or identifiable natural person to whom information relates;
> - '**controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of

personal data; where the purposes and means of such processing are determined by law, the controller may be provided for by that law;

- '**processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- '**recipient**' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not (not including public authorities, who may receive personal data as part of a particular inquiry under the applicable law).

The Parties should consider that a party may have more than one role depending on the processing purpose, and/or may have a role jointly with another party.

A legal basis is needed under the GDPR to allow the sharing of the Data with the Data Recipient. A possible legal basis for sharing personal data where the Requesting User is not the data subject could be consent of the data subjects concerned within the meaning of Article 6(1)(a) or legitimate interest within the meaning of Article 6(1)(f) GDPR. To assess the existence of such a legitimate interest, the obligation to make the data available in accordance with Article 5 of the Data Act may be taken into consideration, although this obligation is not a sufficient legal basis in itself.

2.4 Inaccuracy of declarations

2.4.1 Any Party that becomes aware that any declaration referred to in clauses 2.1 to 2.3 is not, or is no longer, accurate, or will no longer remain accurate in the foreseeable future, must, without undue delay, notify the other Party, unless the other Party is or ought to be already aware of the fact.

If any declaration referred to in clauses 2.1 to 2.3 is not or no longer accurate, the Party should take appropriate steps. In particular, if the Requesting User sold the product and ceases to be the User and the Data Holder receives appropriate information, the Data Holder should terminate the Contract with the Recipient with respect to such User. In the termination notice they should indicate the reason for termination. Merely providing notification would not be sufficient in this case, as there is no way to rectify the situation. If the Data Recipient wishes to continue receiving the Data, they need to approach the new User. However, in some cases the Parties may rectify the infringement of representation. This would be the case, for example, when the User's request is issued by an unauthorised person (e.g. the employee who had no power to represent the user company). In such case, the applicable law may make it possible to validate such action with retroactive effect.

2.4.2 On becoming aware of this situation, the concerned Party must take appropriate action and rectify the inaccuracy of the declaration, to the extent possible. Depending on the circumstances, this may include notifying the Requesting User or any protected third party who is affected or

temporarily suspending the Data being made available by the Data Holder or the use of the Data by the Data Recipient, if making the Data available or the use of the Data has become unlawful.

2.4.3 If the situation is not and cannot be rectified, this Contract must terminate by means of a written termination notice mentioning the reasons for termination given by either Party to the other.

The termination has immediate effect. Where the inaccuracy affects only part of the Data covered by this Contract, termination must take effect only for the relevant part.

Effects of termination are governed by clause 7.3.

3. Making the Data available

3.1 Data covered by the Contract

3.1.1 The Data covered by this Contract consists of the readily available Product Data or Related Service(s) Data within the meaning of the Data Act identified in the request made by the Requesting User in accordance with Article 5 of the Data Act, and includes both non-personal and personal data ('the Data').

The Data are listed in detail in **Appendix 2**.

If, during this Contract, data other than those listed in **Appendix 2** must be made available to the Data Recipient, **Appendix 2** will be amended accordingly.

> The Parties should, in **Appendix 2**, specify the data and metadata covered by the Contract, in compliance with the request made by the Requesting User.
>
> In accordance with Articles 5 and 2(15), (16) and (17) of the Data Act this Data can only be readily available product or related service data:
>
> (a) **Product data** are data generated by the use of the Product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by the User, Data Holder or a third party, including, where relevant, the manufacturer.
>
> (b) **Related service data** are data representing the digitisation of User actions or of events related to the connected product, recorded intentionally by a User or generated as a by-product of a User's action during the provision of the related service.
>
> (c) **Readily available data** are data that the Data Holder can lawfully obtain from the product or related service, without disproportionate effort going beyond a simple operation.
>
> As this Contract lays down the arrangements for making the Data available to the Data Recipient at the request of the Requesting User, these Data are those identified in the request.
>
> The description of the Data must be sufficient to determine which data are covered by a specific regime, if any. In particular, the Parties should set out the details regarding which of the Data qualify as personal data.

3.2 Data characteristics and access arrangements

3.2.1 The Data Holder must make the Data available to the Data Recipient, with the Data having at least the same quality as they did when they became available to the Data Holder, and in any case in a comprehensive, structured, commonly used and machine-readable format as well as the relevant metadata necessary to interpret and use those data.

> 'Metadata' means a structured description of the content or the use of data facilitating the finding or use of those data. In accordance with Article 5(1) of the Data Act, the metadata must be made available with the Data, to the extent that the metadata are '*necessary to interpret and use'* the Data.
>
> Though the relevant metadata needed to interpret and use those data are not laid down and must therefore be identified on a case-by-case basis, the Data Act specifies that '*the data to be made available should include the relevant metadata, including its basic context and timestamp, to make the data usable, combined with other data, such as data sorted and classified with other data points relating to them, or re-formatted into a commonly used format'* (Recital (15) of the Data Act).

3.2.2 The Data Recipient must receive access to the Data

(a) easily and securely;

(b) without undue delay;

(if applicable) (c) continuously and in real time.

3.2.3 In order to meet the requirements of clauses 3.2.1 and 3.2.2, the Parties agree on the specifications set out in Appendix 2.

> In accordance with Article 5(1) of the Data Act, the Data must be made available without undue delay and, where relevant and technically feasible, continuously and in real time.
>
> As there are various ways to implement these legal requirements, the Parties should agree on all the details of how access is to be provided in **Appendix 2**.
>
> In doing so, they should, as a first step, decide whether they want to provide for:
>
> - **full transfer** of the Data, i.e. a copy of the Data is transferred to a medium within the Data Recipient's control:
>   - by way of transmission triggered by the Data Holder (push), such as online transmission, upload into the Data Recipient's cloud space or delivery of a tangible medium on which the Data are stored; or
>   - by way of retrieval triggered by the Data Recipient (pull), such as on being provided with an API, access to the Data Holder's cloud space or similar tools that enable the Data Recipient to access and extract the Data; or
> - **access to the Data where they are stored**, i.e. the Data are accessed and processed on a medium within the control of the Data Holder or a trusted third party, such as by the Data Recipient logging into a dedicated space on the Data Holder's or trusted third party's servers, but the Data are not transferred to a medium within the Data Recipient's control, unless special arrangements are made.

Full transfer gives the Data Recipient maximum liberty, but significantly reduces the Data Holder's ability to prevent abuse.

Access to where the data are stored increases risks for Data Recipients that their business ideas become known, but significantly increases the Data Holder's ability to prevent abuse.

Apart from full transfer and access to where the data are stored, there are further technical possibilities, including access on the Requesting User's device.

If Parties opt for access to where the Data are stored, there are a number of details to resolve, including how to make sure that the Data Recipient's business ideas are not disclosed and what data the Data Recipient is allowed to transfer to a medium within their own control (e.g. derived or inferred data resulting from the Data Recipient's processing activities).

Generally speaking, conditions for access to where the data are stored must not undermine any of the rights afforded to the Requesting User or Data Recipient under the Data Act or other applicable law.

Access to where the data are stored on a medium controlled by a trusted third party will often be preferable over access on a medium controlled by the Data Holder. Access to where the Data are stored should normally still mean remote access, and on-site access should be restricted to extreme situations with the highest degree of sensitivity.

The Parties must also determine the timing of the access to the Data. In accordance with Article 5(1) of the Data Act, when the User so requests, the Data must be made available without undue delay and, where relevant and technically feasible, continuously and in real time.

However, such access is not always needed to achieve the purposes agreed between the Data Recipient and the Requesting User in a specific case. Therefore, the Parties must agree on questions relating to the timing of the access to the Data, such as whether, where relevant and technically feasible, access is provided in real time, and if not at what frequency.

The Parties must also consider a range of further issues, such as what access credentials are required, and which and how many employees of the Data Recipient may access the Data.

3.2.4 If the Data are made available in conformity with the specifications in the Appendix concerning data characteristics and access arrangements, and if it appears that the agreed specifications are insufficient to meet the requirements referred to in clauses 3.2.1 and 3.2.2, the Parties undertake to enter into negotiations in good faith and adapt the specifications so that they meet the agreed requirements.

3.2.5 The Data Holder must provide to the Data Recipient the information necessary for accessing or receiving the Data in accordance with Article 5 of the Data Act.

This includes, in particular, the provision of information readily available to the Data Holder regarding the origin of the Data and any rights which third parties might have with regard to the Data, such as rights of data subjects arising under Regulation (EU) 2016/679 (GDPR), or facts that may give rise to such rights.

The Data Holder specifies this information in **Appendix 2.**

The Parties remain free to agree on any additional support, going beyond the requirements of the Data Act, free of charge or for a fee.

3.2.6 The Data Holder undertakes not to keep any information on the Data Recipient's access to the Data requested beyond what is necessary for:

(a) the sound execution of (i) the Requesting User's access request and (ii) this Contract;

(b) the security and maintenance of the data infrastructure; and

(c) compliance with legal obligations on the Data Holder to keep such information.

3.3 Feedback loops

3.3.1 If the Data Recipient identifies an incident related to clause 3.1 on the Data covered by the Contract or to clause 3.2 on the Data characteristics and access arrangements and if the Data Recipient provides the Data Holder with a detailed description of the incident, the Data Holder and the User must cooperate in good faith to identify the reason for the incident. If the incident was caused by a failure on the part of the Data Holder to comply with their obligations, they must remedy the breach without undue delay. If the Data Holder does not do so, it is considered to be a fundamental breach and the Data Recipient is entitled to invoke clause 8 of this Contract (remedies for breach of contract).

3.3.2 If any of the specifications agreed in accordance with clause 3.2 are impossible or excessively onerous to achieve because of an exceptional change of circumstances occurring after the conclusion of the Contract, the Data Holder must provide the Data Recipient with a detailed description of this and the Parties will enter into negotiations in good faith and adapt the specifications so that they meet the requirements laid down in these clauses. In particular, each Party must provide the other with sufficient information to assess, discuss and resolve the particular situation. This clause does not affect the right of the Data Recipient to invoke remedies in accordance with clause 8.

3.4 Unilateral changes by the Data Holder

3.4.1 The Data Holder may unilaterally change details regarding the specifications of the Data characteristics and access arrangements, if this is objectively justified by the normal conduct of business of the Data Holder – for example by a technical modification due to an immediate security vulnerability in the line of products or related services offered by the Data Holder or

a change in the Data Holder's infrastructure. Any change must meet the requirements of clauses 3.2.

3.4.2 The Data Holder must give notice of the change to the Data Recipient at least (indicate a reasonable period of time) before the change takes effect.

A shorter notice period may suffice:

(a) where the change does not negatively affect data access and use by the Data Recipient; or

(b) where such notice would be impossible or unreasonable in the circumstances, such as where immediate changes are required because of a security vulnerability that has just been detected.

3.4.3 Where the change negatively impacts data access and use by the Data Recipient, the Data Recipient is entitled to terminate the (relevant part of the) Contract without any compensation being due to the Data Holder, this notwithstanding any other rights or remedies the Data Recipient may have.

4. (if the Data must be protected as trade secrets) Protection of trade secrets

1. **Trade secrets sharing** – Data holders cannot, in principle, refuse a data access request under the Data Act solely on the basis that certain data are considered to be protected as a trade secret, as this would subvert the intended effects of the Data Act.

   See clauses 4.1.

2. **Trade secrets** – However, if the Data Holder identifies that certain Data covered by this Contract are protected as trade secrets, as defined by Directive (EU) 2016/943[8] (referred to as the 'Trade Secrets Directive'), they are entitled to certain rights, primarily to continue to preserve the confidentiality of the secrets in question.

   In accordance with Article 2(1) of the Trade Secret Directive, the term 'Trade Secret' means information which meets three requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; and (b) it has commercial value because it is secret; and (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

   A 'Trade Secret Holder' means any natural or legal person lawfully controlling such a trade secret.

   Data can only be identified as trade secrets if they are protected as such by the Data Holder or the Trade Secret Holder when a data access request wasis made in accordance with Article 5 of the Data Act.

   See clause 4.1.1.

3. **Initial identification of trade secrets** – The Data Holders' rights in respect of trade secrets are – initially – only applicable if and to the extent the Data protected as trade secrets are identified in the Contract.

See clause 4.1.2.

4. **During the Contract** – The Data Holders' rights in respect of trade secrets could, however, also apply during the Contract, regarding new data to be made available thereunder.

   See clause 4.1.3.

5. **Audit rights** – In order to preserve the confidentiality of the Data protected as trade secrets, , certain audit rights by means of involving independent third parties are to be considered (while not interfering with the activities of the Data Holder or the Data Recipient), including mechanisms in the case of disagreements related to the results of the audit report.

   See clause 4.2.3.

6. **Trade secret holder rights (1/4)** – The Data Holder (or third-party trade secret holder) may agree with the Data Recipient on requirements to preserve the confidentiality of the trade secrets as a condition for sharing those Identified Trade Secrets – such as taking certain proportionate technical and organisational measures.

   See clauses 4.2 and 4.3,

7. **Trade secret holder rights (2/4)** – If the initial measures do not suffice, the trade secret holder may, on a case-by-case basis, for specific and identified Data protected as trade secrets, either unilaterally increase the level of the measures, or request that additional measures are agreed with the Data Recipient. If there is no agreement on the necessary measures, the Data Holder may suspend the sharing of specific Data protected as trade secrets, under the conditions set out in the Data Act.

   See clause 4.4.2.

8. **Trade secret holder rights (3/4)** – The trade secret holder may also, on a case-by-case basis, refuse to share specific, Identified Trade Secrets, solely in exceptional circumstances and under the conditions set out in the Data Act.

   See clause 4.4.3.

9. **Trade secret holder rights (4/4)** – The trade secret holder may withhold or suspend data sharing, if the Data Recipient breaches their obligations related to the protection of trade secrets.

   See clause 4.4.4.

10. **Retention of Data containing Identified Trade Secrets** – If the Data Holder withholds or suspends data sharing in accordance with clauses 4.4.1, 4.4.2 or 4.4.3, the Data Holder will still be obliged to keep the related Data containing Identified Trade Secret readily available by retaining them until such time as they can be shared within the scope of the Contract.

    See clause 4.5.

11. **Third party identified trade secret holder** – If the trade secret holder is a third party, the Data Holder must make sure that clause 4 also protects their trade secrets and obtain all relevant authorisations by said third-party trade secret holder.

    See clause 4.1.2.

4.1 Applicability of trade secret arrangements

4.1.1 The protective measures agreed in clauses 4.2 and 4.3 of this Contract, as well as the related rights agreed in clauses 4.4, apply exclusively to Data or metadata included in the Data to be made available by the Data Holder to the Data Recipient, which are protected as trade secrets

(as defined in Article 2(1) of the Trade Secrets Directive, held by the Data Holder or another Trade Secret Holder (as defined in Article 2(2) of that Directive).

4.1.2 The identification of data protected as trade secrets and the identity of the Trade Secret Holder are set out in Appendix 4.

The Data Holder declares to the Data Recipient that they have all relevant rights from any third party trade secret holders to enter into this Contract regarding the Data protected as trade secrets.

In accordance with Article 5(9) of the Data Act, '*the data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata*'.

Therefore, the Data Holder should identify the Data protected as trade secrets in **Appendix 4**. However, the Data Holder should not be obliged to describe the trade secret itself. It is sufficient to identify the Data which must be protected to ensure the confidentiality of the trade secret, because the analysis of such Data could reveal the trade secret.

4.1.3 If, during this Contract, new data are made available to the Data Recipient that are protected as trade secrets as set forth in clause 4.1.1, at the request of the Data Holder, Appendix 4 will be amended accordingly.

Until Appendix 4 has been amended and agreed between the Parties, the Data Holder may withhold or temporarily suspend the sharing of the new data protected as trade secrets. In such case, the decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay. The Data Holder shall also notify the competent authority designated under Article 37 of the Data Act. that it has withheld or suspended data sharing and identify which measures have not been agreed or implemented.

4.1.4 The obligations set out in clauses 4.2 and 4.3 remain in effect after any termination of the Contract, unless otherwise agreed by the Parties.

4.2 Protective measures taken by the Data Recipient

4.2.1 The Data Recipient must apply the protective measures set out in **Appendix 4** (hereinafter: 'Data Recipient's Protection Measures').

Parties should, in a separate Appendix, set out all the details of these measures, including for situations when the Data Recipient shares the Data with third parties. Measures may be both technical (e.g. encryption, firewalls, split storage, etc.) and organisational (e.g. internal governance, appropriate identity management and access checks, involvement of a trusted third party).

As the measures need to be proportionate, their content will vary, depending on the nature of the trade secret. The measures will also depend on whether (i) access is to be provided to where the Data are stored or (ii) the Data are to be fully transferred to the Data Recipient. In the former case, the Data Holder has a higher degree of control and can apply part of the protective measures themselves, whereas the Data Recipient may have a lower level of use for the Data. In any case, both Parties will need to focus on achieving the intended effects of the Data Act. For this reason, the various interests need to be balanced, while not subverting those intended effects.

4.2.2 If the Data Recipient is permitted in this Contract and in the contract concluded by the Data Recipient with the User to make the Data available to a third party, the Data Recipient can share the Data protected as trade secrets, if:

(a) they inform the Data Holder without undue delay of the fact that Data protected as trade secrets will be made available to a third party, specify the Data in question, and give the Data Holder the identity, place of establishment and contact details of the third party.

(b) the third party applies the protective measures set out in Appendix 4.

4.2.3 [OPTION] [In order to verify if and to what extent the Data Recipient has implemented and is maintaining the Data Recipient's Protection Measures, the Data Recipient agrees to either (i) annually obtain a security conformity assessment report from an independent third party chosen by the Data Recipient, or (ii) annually allow a security conformity assessment audit from an independent third party chosen by the Data Holder – subject to such independent third party having signed a confidentiality agreement as provided by the Data Recipient. Such security audit report must demonstrate the Data Recipient's compliance with clause 4 and Appendix 4, as applicable at that time. The results of the audit reports will be submitted to both Parties without undue delay.

The Data Recipient may choose between (i) and (ii). If a Party deems the security audit report to be incorrect, they retain the right to obtain a security audit report from another independent third party. If this right is exercised, both independent third-party auditors, together with the Parties, will discuss any difference between those two reports and aim to resolve any pending matters while observing good faith.]

The costs of such audit reports will be born as follows: (*specify the arrangements for the payment of these costs*).

This clause is marked as an option because the Parties may agree other measures in order to verify the User's compliance with their obligations to implement and maintain the Data Recipient's Protection Measures.

4.3 Protective measures taken by the Trade Secret Holder

4.3.1 The Data Holder may apply the measures agreed in **Appendix 4** to preserve the confidentiality of the Data protected as trade secrets (hereinafter: 'Trade Secret Holder's Protection Measures').

4.3.2 The Data Holder may also unilaterally implement appropriate technical and organisational protection solutions, such as software updates, if they do not negatively affect the Data Recipient under this Contract.

4.3.3 The Data Recipient undertakes not to alter or remove the Trade Secret Holder's Protection Measures nor the measures taken in accordance with clause 4.3.2, unless otherwise agreed by the Parties.

4.4 Obligation to share and right to refuse, withhold or terminate

4.4.1 Where the Data Recipient's and Trade Secret Holder's Protection Measures do not materially suffice to adequately protect a particular piece of Data protected as a trade secret, the Data Holder may, by giving notice to the Data Recipient with a detailed description of the inadequacy of the measures request that additional, necessary technical or organisational measures be agreed; if there is no agreement on such measures after a reasonable period of time and if the need for such measures is duly substantiated, e.g. in a security audit report, the Data Holder may withhold or suspend the sharing of the specific Data in question; in such case, the Data Holder must give notice to the Data Recipient and the competent authority designated under Article 37 of the Data Act; notice must be duly substantiated, indicate which measures have not been agreed, where relevant, the trade secrets concerned, and be given in writing without undue delay; the Data Holder must continue to share any Data protected as a trade secret other than these specific Data.

4.4.2 If, in exceptional circumstances, the Data Holder is able to demonstrate that they are highly likely to suffer serious economic damage from disclosure of particular Data protected as a trade secret to the Data Recipient despite the Data Recipient's Protection Measures and, if applicable, the Trade Secret Holder's Protection Measures having been implemented, the Data Holder may suspend sharing the specific Data in question.

They may do so only if they give duly substantiated notice to the Data Recipient and the competent authority designated under Article 37 of the Data Act.

However, the Data Holder must continue to share any Data protected as a trade secret other than those specific Data.

> Refusal or discontinuation of data sharing under Article 5 of the Data Act is limited to exceptional circumstances. Therefore, the notice must be duly substantiated. Aspects to be taken into account can be, for example, the lack of enforceability of trade secrets protection in non-EU countries, the nature and level of confidentiality of the trade secret in question or the uniqueness and novelty of the relevant connected product.

4.4.3 If the Data Recipient fails to implement and maintain their Data Recipient's Protection Measures and if this failure is duly substantiated by the Data Holder, e.g. in a security audit report, the

Data Holder is entitled to withhold or suspend the sharing of the specific Identified Trade Secrets until the Data Recipient has resolved the incident.

In this case, the Data Holder must, without undue delay, give duly substantiated notice in writing to the Data Recipient and the competent authority designated under Article 37 of the Data Act.

4.4.4 Clause 4.4.1 does not entitle the Data Holder to terminate the Contract. Clauses 4.4.2 or 4.4.3 entitle the Data Holder to terminate the Contract only with regard to the specific Identified Trade Secrets, and if:

(a) all the conditions of clause 4.4.2 or clause 4.4.3 have been met;

(b) no resolution has been found by the Parties after a reasonable period of time, despite an attempt to find an amicable solution, including after intervention by the competent authority designated under Article 37 of the Data Act; and

(c) a competent court has not awarded the Data Recipient a court decision obliging the Data Holder to make the Data available and there is no pending court proceedings for such a decision.

4.5 Retention of Data protected as Identified Trade Secrets

4.5.1 Where the Data Holder exercises the right to withhold or suspend the sharing of Data in accordance with clauses 4.4.1, 4.4.2 and 4.4.3, they will need to ensure that the Data in question are retained, so that said Data will be made available to the Data Recipient:

(a) once the appropriate protections are agreed and implemented; or

(b) once a binding decision by a competent authority or court is issued requiring the Data Holder to provide the Data to the Data Recipient.

This retention obligation ends where a competent authority or court in a binding decision allows the deletion of such retained data or where the Contract terminates in accordance with clause 4.4.4.

4.5.2 The Data Holder will bear the necessary costs for retaining the Data under clause 4.5.1. However, the Data Recipient will cover such costs to the extent that the withholding or suspension of Data sharing occurs in accordance with clause 4.4.3.

5. Use of the Data and sharing with third parties

5.1 Permissible use by the Data Recipient

The Data Recipient undertakes to process the Data made available to them under the Contract only for the purposes and under the conditions agreed with the Requesting User.

The Data Recipient must erase the Data when they are no longer necessary for the agreed purpose, unless otherwise agreed with the Requesting User in relation to Data that are non-personal data.

5.2 Sharing of Data with third parties

5.2.1 The Data Recipient must not make the Data available to another third party, unless doing so is contractually agreed with the Requesting User, compatible with any protection measures agreed with the Data Holder and compatible with applicable EU or national law.

The Data Recipient must in any case not make the Data they receive available to an undertaking designated as a gatekeeper under Article 3 of Regulation (EU) 2022/1925 (Digital Markets Act).

5.2.2 Where the Data Recipient is permitted to make Data available to a third party, the Data Recipient must take appropriate contractual, technical and organisational measures to make sure that:

(a) *(if applicable)* the third party applies at least the same protection measures as the Data Recipient must apply under clause 4.2 and respects the protection measures taken by the Data Holder under clause 4.3;

(b) the third party uses the Data exclusively in a way compatible with clauses 5.1 and 5.3;

(c) the Data Holder has at least the same remedies against the third party as against the Data Recipient for use or disclosure of Data prohibited under clause 5.3.

5.2.3 Notwithstanding clauses 5.2.1 and 5.2.2, the Data Recipient may use processing services, e.g. cloud computing services (including Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service), hosting services, or similar services to achieve, for their own account and under their own responsibility, the agreed purposes under clause 5.1. The third parties may also use such services to achieve, for their own account and under their own responsibility, the purposes for which the Data are shared with them.

5.3 Unauthorised use or sharing of Data

5.3.1 The Data Recipient must not:

(a) (for the purposes of obtaining Data) provide false information to the Data Holder, deploy deceptive or coercive means or abuse gaps in the Data Holder's technical infrastructure designed to protect the Data; or

(b) fail to maintain the contractual technical or organisational measures agreed under clauses 4.2 and 4.3; or

(c) alter or remove, without the agreement of the Data Holder, technical protection measures applied by the Data Holder to prevent unauthorised access to the Data and to ensure compliance with this Contract; or

(d) use the Data they received for unauthorised purposes, in violation of clause 5.1; or

(e) use the Data to develop a product that competes with the Product, nor share the Data with a third party for that purpose;

(f) use the Data to derive insights about the economic situation, assets and production methods of the Data Holder, or their use of the Data;

(g) use the Data in a manner that adversely impacts the security of the Product or any Related Service;

(h) use Data for the profiling of natural persons, unless this is necessary to provide the service requested by the Requesting User;

(i) disclose the Data to another third party unlawfully or in violation of clauses 5.2.1 and 5.2.2.

If the Data Recipient does any of these things, this constitutes fundamental non-performance as described in clause 8.1.1 and has the additional consequences described in clause 5.3.2.

5.3.2 In the cases referred to in clause 5.3.1, the Data Recipient must comply, without undue delay, with requests by the Data Holder or the Requesting User to:

(a) inform the Requesting User of the unauthorised use or disclosure of the Data and measures taken to put an end to this;

(b) erase the Data made available by the Data Holder under this Contract, or obtained in an unauthorised or abusive manner, and any copies of it;

(c) compensate the Data Holder, the Requesting User or protected other third party for any harm suffered from the unauthorised use or disclosure; and

(d) end the production, offering, placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through these Data, or the importation, export or storage of infringing goods for those purposes; and

(e) destroy any infringing goods, if (i) there is a serious risk that the unlawful use of the Data will cause significant harm to the Data Holder, trade secret holder or User, or (ii) where this measure would not be disproportionate, given the interests of the Data Holder, trade secret holder or User.

6. Compensation for providing data access

The Parties should, in the Contract itself or in a separate Appendix, determine the details of compensation.

They should agree, at least, on the following:

- the amount of compensation due and the currency;
- the time when payment is due;
- the arrangements for payment.

In accordance with the Data Act, such compensation may always include compensation for the costs incurred in making the Data available. It may also include a margin, except where the Data Recipient is an SME or not-for-profit organisation. It must in any case be reasonable.

In accordance with Article 9(2) of the Data Act, '*(the) costs incurred in making data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage'* as well as, if the compensation includes a margin, '*(the) investments in the collection and production of data, where applicable, taking into account whether other parties contributed to obtaining, generating or collecting the data in question*' must be taken into account to determine the compensation.

Under Article 9(3) of the Data Act, the compensation may also depend on the volume, format and nature of the Data. Under Article 9(7) of the Data Act, the Data Holder must in any case provide information setting out the basis for the calculation of the compensation in sufficient detail, enabling the Data Recipient to assess whether statutory requirements are met.

6.1 (Applicable if the Data Recipient qualifies as an SME/non-profit research organisation)

6.1.1 The Data Recipient declares that they are an SME, as defined in Recommendation 2003/361/EC *or* a non-profit research organisation. They further declare that they do not have partner or linked companies ('enterprises') as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as an SME.

[OPTION] [Evidence of the foregoing is provided in **Appendix 3**.]

6.1.2 The Parties agree that the Data Recipient will compensate the Data Holder [OPTION 1] [as follows: (*specify*)] [OPTION 2] [as specified in **Appendix 3**].

6.1.3 The Data Holder declares that the agreed compensation does not exceed the costs directly related to making the data available to the Data Recipient and which are attributable to the request. These costs include the costs necessary for data reproduction and dissemination via electronic means and storage, but not for data collection or production.

Information setting out the basis for calculating the compensation, enabling the Data Recipient to verify that these requirements are met, is provided by the Data Holder in **Appendix 3**.

6.1.4 The Data Recipient will inform the Data Holder immediately of any changes that call into question their categorisation as an SME.

Where the Data Recipient ceases to qualify as an SME, the Parties undertake to enter into negotiations about the amount of reasonable compensation. If there is no agreement after a reasonable period of time, the Data Holder may suspend the sharing of the Data by giving notice to the Data Recipient.

In this event, the Data Holder must ensure that the Data are retained, so that said Data will be made available to the Data Recipient once the compensation is agreed or a binding decision by

a competent authority or court is issued requiring the Data Holder to provide the Data to the Data Recipient.

The Data Holder will bear the necessary costs for retaining the Data. However, the Data Recipient must compensate the Data Holder for any economic harm suffered because the Data Recipient failed to inform the Data Holder.

6.2 (Applicable if the Data Recipient does not qualify as an SME/non-profit research organisation)

6.2.1 The Parties agree that the Data Recipient will compensate the Data Holder [OPTION 1] [as follows: *(specify)*] [OPTION 2] [as specified in **Appendix 3**].

Information setting out the basis for calculating the compensation, enabling the Data Recipient to verify that these requirements are met, is provided by the Data Holder in **Appendix 3**.

6.2.2 (*applicable in the case of monetary compensation*) If payment of compensation is delayed, the Data Recipient should pay the Data Holder interest on overdue compensation from the time when payment is due to the time of payment, as required by the applicable law.

6.2.3 If the Data Recipient starts to qualify as an SME and informs the Data Holder accordingly, the Parties undertake to modify the amount of the reasonable compensation in accordance with Article 9(4) of the Data Act

7. Date of application, duration of the Contract and termination

7.1 Date of application and duration

7.1.1 This Contract [OPTION 1] [takes immediate effect] [OPTION 2] [takes effect from *(specify date)*].

7.1.2 [OPTION] [This Contract is concluded for [OPTION 1] [an indeterminate period] [OPTION 2] [a fixed period of (*specify)*], subject to any grounds for expiry or termination under this Contract.]

In considering the duration of the Contract, the Parties should be guided primarily by the User's request and the contract concluded between the User and the Data Recipient. If the request is for a **one-off supply** of data, it is sufficient to agree on the data of application.

If the request is for a **continuous supply** of data, the Parties will need to agree on the duration of the Contract and choose either an indeterminate period of time or a fixed period, depending on whether the Requesting User has specified a particular time period.

7.1.3 [OPTION] [The Data Holder must start making the Data available to the Data Recipient [OPTION 1] [without undue delay after the Contract has come into effect] [OPTION 2] [on *(specify date and, where applicable, further details as to timing)*].]

> Normally, the Parties will want performance to start right after the Contract has come into effect. But this is not necessarily the case, e.g. if one or both Parties still has/have to prepare for performance to start.

7.2 Termination

7.2.1 Irrespective of the contract period agreed under clause 7.1.1, and without prejudice to clause 2.4.3, this Contract terminates:

(a) upon the destruction of the Product or permanent discontinuation of the Related Service, or when the Product or Related Service loses its capacity to generate the Data in an irreversible manner; or

(b) when both Parties so agree.

7.2.2 The Data Recipient may terminate the Contract at any time during the contract period by giving the Data Holder a notice of (*insert period)*. The Data Recipient must notify the Requesting User that the Contract has been terminated.

[OPTION] Where the Data Recipient terminates the Contract under this clause before (*insert point in time or minimum contract period)*, they must compensate the Data Holder for the costs incurred by the Data Holder for making the Data available, as follows: *(specify)*.

> There may be cases where the Data Holder incurs expenses to make the Data available to the Data Recipient, such as by adapting their digital infrastructure, trusting these expenses will be amortised over time.
>
> In this case, the Data Holder may want to make sure that they receive compensation from the Data Recipient.

7.3 Effects of expiry and termination

7.3.1 Expiry of the contract period or termination of this Contract releases both Parties from their obligation to effect and to receive future performance but does not affect the rights and liabilities that have accrued up to the time of expiry or termination.

Expiry or termination does not affect any provision which is to operate even after the Contract has come to an end, in particular any limitations on the permissible use and sharing of the Data

by the Data Recipient under clause 5, clause 4 on trade secrets, clause 9.1 on confidentiality, clause 9.5 on applicable law and clause 9.7 on dispute resolution.

7.3.2 [OPTION 1] [The Data Holder must take appropriate exit support measures as the Data Recipient may reasonably expect.] [OPTION 2] [The Data Holder must take the following exit support measures: *(specify)*]

Parties may consider whether the Data Recipient requires any exit support measures.

This will be relevant, for example, if the Data Recipient was allowed to extract Data from a medium controlled by the Data Holder but had not yet extracted the data because they did not expect the Contract to be terminated.

8. Remedies for breach of contract

Parties may wish to agree not only on the data-specific rights and obligations (many of which already follow from the Data Act) but also on matters of general contract law – such as the rights and remedies of a contracting party where there is non-performance on the part of the other contracting party.

For such matters of general contract law, the Parties may wish to rely on statutory default rules, or on other contract templates.

If they wish to use these model contractual terms, they should make sure they are compatible with any mandatory national law that may be applicable to the Contract.

8.1 Cases of non-performance

8.1.1 A non-performance of an obligation by a Party is fundamental if:

(a) the non-performance substantially deprives the other Party of what they were entitled to expect under this Contract, unless the non-performing Party did not foresee and could not reasonably have foreseen that result; or

(b) it is clear from the circumstances that the non-performing Party's future performance cannot be relied upon.

8.1.2 A Party's non-performance is excused if it is due to an impediment beyond their control and if that Party could not reasonably have been expected to take the impediment into account at the time of the conclusion of this Contract, or to have avoided or overcome the impediment or its consequences.

Where the impediment is only temporary, the excusing of the Party's non-performance has effect for the period during which the impediment exists. However, if the delay amounts to a fundamental non-performance, the other Party may treat it as such.

The non-performing Party must ensure that notice of the impediment and of its effect on their ability to perform is received by the other Party without undue delay after the non-performing Party knew or could reasonably be expected to have become aware of these circumstances. The other Party is entitled to damages for economic harm resulting from the non-receipt of such notice.

8.2 Remedies for non-performance

8.2.1 In the case of a non-performance by a Party, the other Party shall have the remedies listed in the following clauses, without prejudice to any remedies available under applicable law.

8.2.2 Remedies which are not incompatible may be cumulated.

8.2.3 A Party may not resort to a remedy to the extent that they cause the other Party's non-performance, such as where a shortcoming in their own data infrastructure did not allow the other Party to duly perform their obligations. A Party may also not rely on a claim for damages suffered to the extent that they could have reduced the damage by taking reasonable steps.

8.2.4 The aggrieved Party can:

(a) request that the non-performing Party complies, without undue delay, with their obligations under this Contract, unless it would be unlawful or impossible or unless specific performance would cause the non-performing Party costs which are disproportionate to the benefit the other Party would obtain;

(b) withhold their own performance under this Contract, unless this would foreseeably cause a detriment to the non-performing Party that is obviously disproportionate in the light of the gravity of the non-performance (if applicable) [provided that all conditions set out in clause 4.4.4 are met, if the Data Recipient fails to implement or maintain the Data Recipient's Protection Measures agreed in clause 4.2.1];

(c) terminate the contract with immediate effect without penalty, by giving notice to the other Party, if:

(i) the other Party's non-performance is fundamental; or

(ii) in the case of non-performance which is not fundamental, the aggrieved Party has given notice fixing a reasonable period of time to remedy the non-performance and the period has lapsed without the other Party performing;

(iii) *(if applicable)* [provided that all conditions set out in clause 4.4.5 are met, in cases described in clauses 4.4.2 or 4.4.3;]

(d) claim damages for economic harm caused to them by the other Party's non-performance which is not excused under clause 8.1.2; the non-performing Party is liable only for damage which they foresaw or could be reasonably expected to have foreseen at the time of conclusion of this Contract as a result of their non-performance, unless the non-performance was intentional or grossly negligent.

8.2.5 [OPTION] Where a Party fails to perform their obligations under this Contract they shall, in any case, pay the penalties set out in detail in **Appendix 5**, which the Parties deem to be damages within the meaning of clause 8.2.4 (d). The non-performing Party has the right to request that

the penalty is reduced to a reasonable amount if they can prove that the penalty is grossly excessive in relation to the damage resulting from the non-performance.

> The Parties may wish to establish penalties for specific types of non-performance as it may be too onerous for the aggrieved Party to prove the amount of actual damage caused by, for example, a failure to supply Data. Penalties should be proportionate.

9. General provisions

9.1 Confidentiality

9.1.1 The following information must be considered confidential:

(a) information referring to the trade secrets, financial situation or any other aspect regarding the operations of a Party, unless that Party has made this information public;

(b) information setting out the basis for the calculation of the reasonable compensation;

(c) information referring to the Requesting User and any third party, unless they have already made this information public.

9.1.2 Both Parties agree to take all reasonable measures to store securely confidential information and not to make available such information to any third party, unless:

(a) one of the Parties is under a legal obligation to make available the relevant information, e.g. in order to comply with the obligation to provide information showing that there has been no discrimination in accordance with Article 8(3) of the Data Act; or

(b) it is necessary for one of the Parties to make available the relevant information in order to fulfil their obligations under this Contract; or

(c) one of the Parties has obtained the prior consent from the other Party or the party providing the confidential information or affected by its disclosure.

9.1.3 In any case, the Data Holder may disclose or make available [OPTION 1] [the Contract to the Requesting User] [OPTION 2] [such information to the Requesting User as is necessary for the Data Holder to demonstrate compliance with their obligations (i) in respect of the Data Recipient

under Article 5 of the Data Act or (ii) resulting from a contract made with the Requesting User under Article 4(6) of the Data Act].

9.1.4 These confidentiality obligations remain applicable after the termination of the Contract for a period of *(specify the period)*.

9.1.5 These confidentiality obligations do not remove any more stringent obligations under (i) the GDPR, (ii) the provisions implementing Directive 2002/58/EC or Directive (EU) 2016/943 or (iii) any other Union law or Member State law.

9.2 Non-discrimination

The Data Holder declares that the terms of this Contract and any practices related to its fulfilment do not discriminate between comparable categories of Data Recipients, including any of their partner or linked ('enterprises'), as defined in Article 3 of the Annex to Recommendation 2003/361/EC, when making data available.

If the Data Recipient considers the conditions under which data have been made available to them to be discriminatory, the Data Holder must, on request by the Data Recipient, provide without undue delay information showing that there has been no discrimination.

9.3 Means of communication

Any notification or other communication required by this Contract must be in writing and may be delivered by hand, sent by prepaid post, or transmitted by electronic means, including email, provided that the sender retains proof of sending to the addresses listed below:

Party	**Contact Person**	**Email**	**Phone**	**Address**
User	[Name]/[Position]	[Email]	[Phone]	[Address]
Data Recipient	[Name]/[Position	[Email]	[Phone]	[Address]

Any such notice or communication will be deemed to have been received:

(a) if delivered by hand, on the date of delivery;
(b) if sent by prepaid post, on the third business day after posting;
(c) if sent by electronic means, on the date of transmission, provided that no error message indicating failure to deliver has been received by the sender.

9.4 Entire Contract, amendments and severability

9.4.1 This Contract (together with its **Appendices** referred to in the Contract) constitutes the entire Contract between the Parties with respect to the subject of this Contract and supersedes all prior

contracts and understandings between the Parties, oral or written, as regards the subject of this Contract.

9.4.2 Any amendment to this Contract will be valid only if agreed to by the Parties in writing, including in any electronic form.

9.4.3 If any provision of this Contract is found to be void, invalid, voidable or unenforceable for whatever reason, and if this provision is severable from the remaining terms of the Contract, these remaining provisions will continue to be valid and enforceable. Any resulting gaps or ambiguities in this Contract must be dealt with in accordance with clause 9.6.

9.5 Applicable law

This Contract must be governed by the law of *(specify state)*.

9.6 Interpretation

9.6.1 This Contract is concluded by the Parties against the background of the Parties' rights and obligations under the Data Act. Any provision in this Contract must be interpreted so as to comply with the Data Act and other Union law or national legislation adopted in accordance with Union law, as well as any applicable national law that is compatible with Union law and cannot be derogated from by agreement.

9.6.2 If any gap or ambiguity in this Contract cannot be resolved in the way referred to in clause 9.6.1, this Contract must be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 9.5).

9.7 Dispute settlement

9.7.1 The Parties agree to use their best efforts to dissolve disputes amicably and, before bringing a case before a court or tribunal, to submit their dispute to *(insert name and contact details of a particular dispute settlement body or, for disputes within its competence, refer to any dispute settlement body in a Member State that meets the conditions of Article 10 of the Data Act)*.

9.7.2 [OPTION] [The courts of *(specify state)* will have exclusive jurisdiction to hear the case concerning this Contract.]

Appendix 1 (evidence on the request and, if applicable, any mandate)

[To be drafted by the Parties]

Appendix 2 (details of the Data covered by the Contract and of access arrangements)

In this Appendix, the Parties should give the details of the data covered by the Contract, of access arrangements and of the means and information necessary to access and use the Data, as agreed in clauses 3.1 and 3.2.

This Appendix merely contains a list of key elements that the Parties should agree on. Both its form and its content is to be adapted by the Parties, so that it fits their needs. The Parties can, in particular, add to this list.

A. Specification of content of the Data

The Appendix should sort and list the Product Data and Related Service(s) Data covered by the Contract, indicating the content of the Data and the collection frequency (structured list of data points or precise categories of data).

B. Duration of retention

The Appendix should indicate the duration of retention, so that the User is informed about the duration of the availability of the Data. They may do so in a granular manner for each data point or group of data points.

C. Data regime

The Appendix should specify here whether all or part of the Data are particular data regulated by a specific regime. The Appendix could, for example, indicate whether and what Data qualify as personal data.

D. Data structure and format

The Appendix should specify here in what structured, commonly used and machine-readable format the Data are made available.

E. Transfer/access medium

The Appendix should specify here via what secure and convenient electronic medium the Data will be made available by the Data Holder to the Data Recipient, either by transfer or access.

F. Timing of access to Data

The Appendix should specify the rate, frequency, and other time-related parameters of access to the Data, such as, for instance, real-time, near-real-time, continuously, without undue delay, in a certain frequency.

G. Starting date

The Appendix should specify the starting date on which the Data Holder will make the Data available to the Data Recipient.

H. Information necessary for the exercise of the Data Recipient's access rights

The Appendix can specify here the information necessary to enable the Data Recipient to exercise their access rights. It may include a contact person to resolve technical issues, on the Data Holder's side as well as on the Data Recipient's side.

Appendix 3 (evidence on the size of the Data Recipient and details of the calculation of compensation)

[To be drafted by the Parties]

Appendix 4 (Trade Secrets)

[To be drafted by the Parties]

ANNEX V: MODEL CONTRACTUAL TERMS
for contracts for voluntary sharing of data between Data Sharers and Data Recipients

These model contractual terms are designed for contracts where the data sharing is voluntary between a Data Sharer and a Data Recipient, i.e. the Data Sharer is not obliged to share data under Regulation (EU) 2023/2854 (referred hereto as the 'Data Act'). or under any other legal obligation contained in Union law (such as Articles 6(9) and 6(10) of the Digital Market Act) or national law.

The main novelty of the Data Act for such relationships is that it contains in its Article 13 an unfair contract terms control. Contractual terms concerning access to and use of the data, or liability and remedies for a breach or the termination of data-related obligations, which have been imposed unilaterally on an enterprise by another enterprise, are non-binding if they are unfair.

While this Contract is not meant to replace contracts on voluntary data sharing which already exist, it can be used as a benchmark for assessing the fairness of clauses in existing contracts.

In cases of mandatory data sharing of product data and related service data under the Data Act, please use either the '*Model Contractual Terms for contracts between Data Holders and Data Recipients on the making available of data upon the request of users of connected products and related services*' (Article 5 of the Data Act) or the *'Model Contractual Terms for contracts on data access and use between Data Holders and users of connected products and related services'* (Article 4 of the Data Act).

Other mandatory data-sharing scenarios should be dealt with separately by the Parties, making sure that both obligations under the specific legal rule and obligations under Chapter III of the Data Act are complied with. Dedicated sets of terms developed by the European Commission or a Member State may apply to a mandatory data-sharing scenario of this kind.

1. Parties to the Contract

This Contract on the access to and use of data is made between

(insert name, contact details and further references) ('Data Sharer')

and

(insert name, contact details and further references) ('Data Recipient')

referred to in this Contract collectively as 'the Parties' and individually as 'the Party'.

A **Data Sharer** can be any enterprise that:

- is holding data, and
- has the right to make data available on a voluntarily basis, and
- controls, depending on the case, the characteristics of the data or the means of access to the data, in such a manner that they can comply with the obligations provided for in these model contractual terms (if this is not the case, another contract could be more appropriate).

Please note that for sharing personal data, compliance with applicable data protection law is required (including the need for a legal basis, and, where data is shared with a Data Recipient in a third country, compliance with the requirements for international data transfers).

For Data Act-related use-cases, the Data Sharer could be for example:

- a Data Holder under Article 2(13) of Regulation (EU) 2023/2854 who has the right to share product data and related services data or who wants to share derived or inferred data;
- a User of a connected product or related service to whom data were transferred by a Data Holder (including, for example data, from a virtual assistant interacting with the product or related service);
- a former Data Recipient under Article 2(14) of Regulation (EU) 2023/2854 who now has the right to use and make data available in accordance with its agreements with the user and Data Holder.

For other use-cases, the Data Sharer could be for example:

- a farmer who wants to share soil data for the improvement of their plants patterns with their AI-provider or for the training, improvement or development of new AI-systems with another AI-provider;
- a company which wants to sell parts of its business data to another business;
- a university which wants to sell data to a sociological research institute to create statistics;
- an IT-company which wants to participate in a data network for cybersecurity incidents to foster incident response timing

A **Data Recipient** can be any enterprise to which the Data Sharer makes data available, and which receives and uses the data for its own business purposes within the scope of this Contract as the counterparty of the Data Sharer.

The definition of Data Recipient in this Contract covers any receiving party of any type of data sharing, not just Data Recipients within the mandatory data sharing scenarios under the Data Act.

2. Data covered by the Contract

The data covered by this Contract consists of the Data identified in **Appendix 1** ('the Data'). Should all or part of the Data provided under this Contract be covered by a specific regime (except for personal data as specifically addressed under clause 3.2), the Data Sharer commits to identifying such Data in **Appendix 2**, as well as to taking appropriate measures to protect such Data in accordance with the applicable regime.

Identification of specific regimes

As these terms relate to purely voluntary data sharing, the Data Sharer has no obligation to share any data which would be covered under a special legal regime (especially and contrary to mandatory data sharing under the Data Act, there is no obligation to share data protected as trade secrets). If the data under the specific regime are not shared, they do not need to be listed in **Appendix 2**; if they are shared however, they must be listed and protected accordingly.

Data identified as such in **Appendix 2** may be for example:

- protected as a trade secret by the Data Sharer, in which case they will be covered under the clause on 'Trade Secrets';

- considered to be confidential by the Data Sharer, in which case they will be protected under the clause on 'Confidentiality';
- protected by the sui generis database rights or any other intellectual property rights, in which case the clause on 'Intellectual Property' will apply;
- covered by a sector-specific regulation (e.g. energy, defence, security, finance, clinical investigations, etc.), including regulations related to common European Data Spaces;
- impacted by competition law restrictions; or
- protected by any other relevant legal regime that the Parties would like to highlight.

The description of the Data covered by the relevant legal regime should be completed with information necessary for legal and safe use of the Data by the Data Recipient (for example in the case of IP protection, licensing information and third-party copyright).

The specific case of common European data spaces

In some situations, data could be shared within the context of a domain-specific common European Data Space. This data sharing should be implemented in accordance with the provisions of the relevant Regulation applicable to such Data Space, when mandatory data sharing under such a Regulation is concerned. Outside the scope of mandatory data sharing under the relevant Regulation applicable to a Data Space, voluntary data sharing remains possible. In this case, this set of terms can be used.

3. Basis for the Contract

3.1 Origin of the data

3.1.1 The Data Sharer hereby declares that Data provided under this Contract originates from the following sources: *(Please specify all sources of Data and, if possible, Data provided by each source)*

Parties can specify different kinds of sources, such as, for example:

- product data or related service data under the Data Act;
- other data coming from a product or related service which do not qualify as product data or related service data under the Data Act (e.g. derived data or data coming from another software, such as demographic data entered in an app by its user);
- data coming from external sources, for example data provided to the Data Sharer by a third party in relation to such third party's products or users;
- data created by the Data Sharer (autonomously), for example customer records created by the employees of the Data Sharer in its Customer Relationship Management system, tables, processed data, inferred data, derived data, merged data, etc.

Warranties are generally the consequences of the Data Sharer providing the Data and the Data Recipient being unable to verify the legality of such Data and their origin. In such cases, the Data Recipient needs to rely on the Data Sharer and may wish to obtain certain warranties in that regard. However, warranties may not be relevant in the situation where the Data Recipient is better placed to verify and/or take the risk regarding the Data – for example – due to the fact that the Data Sharer is an SME and/or that the Data are retrieved directly from the product.

3.1.2 The Data Sharer declares that:

(a) *(If applicable)* as the Data contains non-personal product or related service data (as defined in Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data ('Data Act')) and the Data Sharer under this Contract has access to the Data in its capacity as a Data Holder, the processing and sharing of such Data is, in accordance with Article 4(13) of the Data Act, subject to a contract with the respective user as defined under Article 2(12) of the Data Act" ("User"), and that this Contract allows the Data to be shared for the purposes considered under this Contract;

(b) *(If applicable)* as the Data contains product or related service data and the Data Sharer under this Contract has gained access to it in its role as a Data Recipient under Article 5 of the Data Act, this Contract is not in breach of contractual commitments with the User and the Data Holder and obligations under the Data Act;

(c) it owns or possesses sufficient legal and/or contractual rights to the Data without any violation or infringement of the rights of others and there is no action, suit or proceeding pending against the Data Sharer which, if adversely determined, would have a material adverse effect upon its ability to grant the rights granted hereunder;

(d) except as otherwise specified in **Appendix 2** and without prejudice to clause 3.2, they have obtained and will maintain for the duration and purpose of the Contract, at their own cost, all permissions, licences and authorisations required for sharing and use by the Data Recipient of any Data obtained from or provided by a third party.

3.1.3 (*if applicable)* As the Data contains product or related service data (as defined in the Data Act) and the Data Sharer under this Contract has gained access to it in accordance with Article 4 of the Data Act in their role as a User, the Data Recipient declares that they are not designated as a gatekeeper pursuant to Article 3 of Regulation (EU) 2022/1925 ('Digital Markets Act').

3.1.4 [OPTION] [Each Party shall ensure that all Data, files, or software transmitted to the other Party under this Contract are free from any viruses, malware, ransomware, or other harmful code that could compromise the integrity, security, or functionality of the other Party's systems.]

3.1.5 [OPTION] [Each Party shall ensure that all Data, files, or software transmitted to the other Party under this Contract stem from data collection activities which comply with applicable *(specify: professional-, ethical industry-, cybersecurity-, research- and/or AI-)* standards.]

3.2 Compliance with data protection and privacy law

3.2.1 Insofar as the Data qualifies as personal data, each Party declares that they comply with the Regulation (EU) 2016/679 ('GDPR') and, where relevant, Directive 2002/58/EC, as well as any other applicable data protection law.

3.2.2 The Parties must list in **Appendix 3** the details as to which Data qualify as personal data, as well as the respective obligations of the Parties with regard to the processing of such personal data under this Contract.

Roles of the parties and agreements under the GDPR

The concept of 'personal data' under the GDPR is very broad. It captures any data that relates to an identified or identifiable person. Non-personal data, can become personal data for example when they are part of a mixed dataset, where they are combined with new data and the outcome of this combination makes it possible to link the data to an identified or identifiable individual. This can also happen where new data-processing capabilities emerge. Parties should assess their own roles under the GDPR.

Key concepts of the GDPR:

- 'data subject' is the identified or identifiable natural person to whom information relates;
- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data;
- 'processor' is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

These clauses apply when the Data Sharer is a controller or a joint controller with another party under the GDPR. To determine who has what kind of role under the GDPR, Parties must consider if they are deciding why (purpose) and how (which means to use) the personal data are processed.

- If the Data Sharer shares Data with the Data Recipient who uses the Data for their own purposes, both Parties are separate controllers and bear their own responsibility for complying with the GDPR.
- If the Data Sharer shares Data with the Data Recipient in order to pursue a joint purpose, the Data Sharer and the Data Recipient are joint controllers under Article 26 GDPR. They must jointly arrange how they comply with the GDPR.
- Where additional contractual clauses are needed to ensure compliance with the GDPR,(e.g. under Article 26 or Article 46), such clauses can (and should) be used together with these model contractual terms. The parties can refer to them in **Appendix 3**, which should generally specify how the requirements set out in the GDPR are fulfilled, including with regard to the respective roles and responsibilities of the Parties under the GDPR.

Valid legal basis

A valid legal basis under Article 6(1) GDPR to share the data should exist and the data subject has to be informed about that (further) processing under Article 13 or 14 GDPR.

- A valid legal basis for the Data Sharer and Data Recipient acting as two separate or joint controllers could be consent of the data subject concerned, a contract with or in the interest of the data subject concerned or the legitimate interest of the controller(s) or a third party (provided that it is not overriden by the interests or rights of the data subject concerned).
- Data can only be shared for a specified, explicit and legitimate purpose. This could be, for example, data sharing for the purpose of improving the product, where the parties agreed to use the data to jointly develop a new functionality.
- A Data Sharer acting as a controller could also share – on the basis of their legitimate interest to better retain clients in the future – the data with their mother company also acting as an independent data controller and using the data to create global statistics – on the basis of their legitimate interest to improve the services globally provided by the group.

The Data Recipient should receive sufficient information from the Data Sharer to be able to demonstrate their compliance with the GDPR. For example, the Parties can agree to mention in **Appendix 3** the original purpose for collecting the Data. This can be necessary to ascertain whether

processing for another purpose is compatible with the purpose for which the personal data have initially been collected under Article 6(4) GDPR in the case of joint controllership. All the necessary details about the respective obligations of the Parties with regard to the processing of such personal data under this Contract should be specified in **Appendix 3**.

More information on the GDPR:

- Explanation of key concepts of the GDPR:

  https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en

- Data protection guide for small businesses:

  https://www.edpb.europa.eu/sme-data-protection-guide/home_en

- European Data Protection Board guidelines, recommendation and best practices:

  https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

- You may find additional guidance by national data protection authorities in each Member State. List of national data protection authorities:

  https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

- Standard contractual clauses under Article 28 GDPR:

  https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en

- Information when transferring personal data outside the EU/EEA:

  https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

3.3 Inaccuracy of declarations

3.3.1 Any Party that becomes aware that any declaration referred to in this clause is not, or no longer, accurate, or will no longer remain accurate in the foreseeable future, shall, without undue delay, notify the other Party, unless the other Party is or ought to be already aware of the fact.

3.3.2 On becoming aware of this situation, the concerned Party must take appropriate action and rectify the inaccuracy of the declaration, to the extent possible. If the situation is not and cannot be rectified, this Contract must terminate by means of a written termination notice mentioning the reasons for termination given by either Party to the other. The termination has immediate

effect. Where the inaccuracy affects only part of the Data covered by this Contract, termination must take effect only for the relevant part.

3.3.3 Further effects of termination are governed by clause 9.3.

4. Making the data available

4.1 Data characteristics

The Data Sharer can make various degrees of commitment regarding the Data provided, from the most basic commitment that it will be provided with the metadata, making it intelligible, to the most stringent commitment that it will fit the purposes contemplated by the Data Recipient and/or be exhaustive and accurate. The Parties could select options among the following.

It is moreover possible for the Parties to add any additional requirement which makes sense from the perspective of the specific data sharing situation: for example, when Data are shared for research purposes, the objective of research reproducibility may require that the frequency and retention period of each updated dataset version is specified, in which case these elements can be added in the section 'specific quality requirements' below.

The Data Sharer shall make the Data available to the Data Recipient:

(a) in the same quality as it is available to the Data Sharer; and

(b) together with the relevant metadata, domain tables, semantics, licensing information and other information required in order to make the Data intelligible to the Data Recipient.

[OPTION] [and *(Please select, if applicable, one or more options as appropriate)*

- ☐ The Data are made available in a comprehensive, structured, commonly used and machine-readable format. The Parties consider this requirement to be fulfilled by the following specifications concerning the Data: *(Please specify)*
- ☐ The Data are made available in accordance with the FAIR (Findable, Accessible, Interoperable, Reusable) principles as further described in www.go-fair.org/fair-principles: *[OPTION]* [*(Please describe how to meet the FAIR-criteria)*]

Adherence to the FAIR principles can be achieved by meeting several measurable requirements. The RDA FAIR maturity model (https://publications.jrc.ec.europa.eu/repository/handle/JRC140764) provides a framework for assessing the extent to which these indicators are met. A Data Sharer should align their data-sharing practices with a maturity level appropriate to their specific needs.

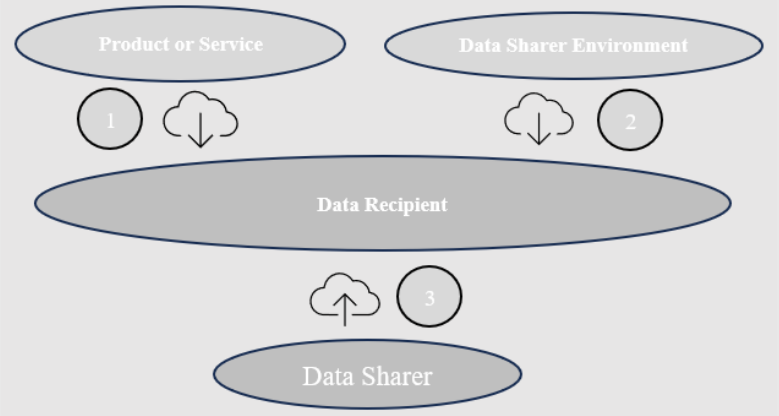
At a minimum, the Data Sharer must ensure that metadata are available and meet all indicators flagged as 'essential' by the maturity model. Additionally, a Data Sharer may use context-specific tools, good practices and guidelines, such as those available at https://doi.org/10.2760/5646214, to simplify and concretise the implementation of FAIR principles.

- ☐ The Data are adapted to the following context of processing by the Data Sharer in accordance with the usual expectations: *(Please add a brief description)*

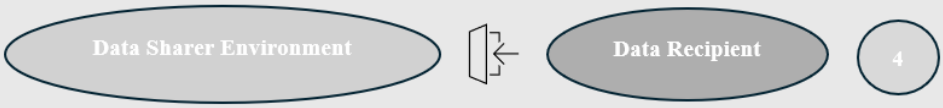
- ☐ The Data are fit for the objectives pursued by the Data Recipient: *(Please add a brief description)*
- ☐ The Data Sharer shall make the following available to the Data Recipient: *(Please add/remove/complete specific quality requirements)*
  - An exhaustive dataset, i.e. the Data contain all the Data in the Data Sharer's possession within the scope of this Contract; and/or
  - An up-to-date dataset, i.e. the Data reflect the Data in the Data Sharer's possession on the date on which this Contract is signed; and/or
  - An accurate dataset, i.e. the Data have been curated by the Data Sharer and are – to the best of its knowledge – error free, correct and reliable; and/or
  - A dataset which is compliant with the following standards: *(specify, e.g. interoperability, accessibility, security, etc.)*
  - A dataset available in a format which is open, meaning a format which is not proprietary and can be used by anyone, namely: *(specify)*].

4.2 Obligations of the Data Sharer in relation to access to the Data

The Data Sharer may make the Data available in different ways, either by giving or retaining technical control of the Data (without prejudice to intellectual property rights granted or retained). For example, the Parties may agree that the Data Recipient retrieves the Data either directly from the product/service (Option 1) or from the environment of the Data Sharer (Option 2), or that the Data Sharer oversees the transferring of Data to the Data Recipient (Option 3).



The parties may also agree that the Data will not be transferred to the Data Recipient but will be made available for processing in the Data Sharer environment. This would be especially relevant in a situation involving personal data (Option 4).



When making Data available under one or more of these options, different data security measures need to be implemented by the Parties to ensure initial and ongoing confidentiality, integrity and availability of the Data. Besides legal safeguards regarding personal data that are described in 3.2. (respectively in **Appendix 3**), security measures (as further described in **Appendix 4**) should also cover technical and organisational aspects regarding, for example:

- data confidentiality by access control and secure data flow;
- data retention and deletion provisions;
- data integrity measures and monitoring measures;
- data breach provisions.

4.2.1 The Data Sharer shall make the Data available to the Data Recipient by *(Please select all options that apply)*:

☐ **[OPTION 1: Retrieval by the Data Recipient from products or service]** enabling retrieval directly from the following products and/or services not hosted by the Data Sharer, including by making available any required technical specifications (e.g. communication protocol) under the following technical conditions: *(Insert method and products/services not hosted by the Data Sharer);*

☐ **[OPTION 2: Retrieval by the Data Recipient from the environment of the Data Sharer**] enabling retrieval from the Data Sharer's environment, including by making available any required technical specifications, under the following technical conditions: *(Insert method, e.g. file download or using the API (Application Programming Interface) to interact with the Data Sharer's services);*

(Applicable if OPTION 1 or OPTION 2 are chosen) [The Data Sharer hereby authorises the Data Recipient to use the specifications for the purpose of retrieving the Data solely as defined in this Contract. Except for the above-mentioned right, the Data Recipient hereby agrees and acknowledges that they shall have no other right to, interest in or licence for the specifications.]

☐ **[OPTION 3: Transfer by the Data Sharer to the environment of the Data Recipient**] ensuring the full transfer of the Data from the environment of the Data Sharer to the environment of the Data Recipient, under the following technical conditions: *(Insert method, e.g. one-time transfer or regular transfers of zip files to the Data Recipient);*

☐ **[OPTION 4: Access by Data Recipient to the environment of the Data Sharer]** [providing access to the Data in the Data Sharer's environment under the following technical conditions: *(Insert method, e.g. logging into a platform, allowed functions including export functions, as the case may be);*

The Data Sharer hereby grants the Data Recipient the non-transferable, non-sublicensable right to access the Data in the environment described above only for the purpose and the duration specified in this Contract. The Data Sharer reserves the right to suspend access to the environment if non-compliant use is detected.]

4.2.2 For the purpose of clause 4.2.1, the environment of the Data Sharer and the environment of the Data Recipient shall be deemed to include:

(a) the environment of any third party designated by the concerned Party to hold or receive the Data on their behalf (including, as appropriate, any secure processing environment as defined under Article 2(20) of Regulation (EU) 2022/868);

(b) any application or software hosted by the concerned Party directly or via the use of service providers.

> In cases where machine learning or AI applications are to be developed, novel technologies such as Federated Learning and Differential Privacy, as further described in https://publications.jrc.ec.europa.eu/repository/handle/JRC141298, can be used to ensure that data are accessed by the Data Recipient in a privacy-preserving manner.
>
> In the case of Federated Learning, the data are 'visited' by the algorithm of the Data Recipient, which is executed within the secure processing environment of the Data Sharer or a third party. This approach prevents the Data Recipient from having direct access and visibility of the data. In the case of Differential Privacy, noise is added to the original data to protect certain sensitive features.

4.2.3 The Data Sharer shall make the Data available to the Data Recipient in conformity with the following timing requirements/calendar: (*Insert timing, e.g. daily, specific time, frequency, real time) and/or detailed calendar or time limit*)

[OPTION] [If, during the term of this Contract, the Data Sharer comes into possession of an updated or corrected version of the Data, it commits to making such updated or corrected version available to the Data Recipient without undue delay after it becomes available to the Data Sharer. Where the Data are continuously updated and corrected, they will be made available to the Data Recipient *(specify: daily / weekly / monthly)*.]

[OPTION] The Data Sharer will ensure that each new version of the dataset is correctly labelled, and that previous versions remain available to the Recipient for the duration of the Contract and for a period of *(specify)* thereafter.

[OPTION] The Data are retained by the Data Sharer for a duration of *(specify)*, after which they will no longer be accessible to the Data Recipient.

4.2.4 The Data Sharer must provide the Data Recipient with the means and information necessary for accessing or receiving the Data in accordance with this Contract. This includes, in particular:

(a) [OPTION where the data are not provided in a standard format] [the provision of software and an accompanying licence required for using the Data for the agreed purpose that is not readily available on the market but could be provided by the Data Sharer and/or mapping from the available format to an open and commonly used specification/vocabulary;]

(b) the provision of information readily available to the Data Sharer regarding the origin of the Data and any rights which third parties might have with regard to the Data, or facts that may give rise to such rights.

[OPTION] The Parties hereby agree that these means and information include the following: *(specify)*.

4.3 Obligations of the Data Recipient in relation to access to the Data

4.3.1 The Data Recipient shall provide the Data Sharer with the technical information and the relevant Data required for the fulfilment by the Data Sharer of the requirements set out above.

4.3.2 (If applicable in the case of access to the Data in the Data Sharer's environment) The Data Recipient:

(a) will ensure that only employees who work for or with the Data Recipient and whose duties necessitate access for the performance of this Contract ('need-to-know principle') may access the Data Sharer's environment and such employees will comply with this Contract, its appendices and applicable legislation;

(b) will not:

(i) authorise or enable any third party to access the Data Sharer's environment;

(ii) create derivative works or access the Data Sharer's environment to develop any competing product or service or to copy any element, function or graph within the Data Sharer's environment;

(iii) copy, replicate, reverse engineer, decompile, disassemble, or attempt to extract any source code, algorithms, methods, or techniques used in the Data Sharer's environment [OPTION] [except to the extent strictly required for compatibility testing or optimisation for integration];

(iv) circumvent or bypass any security mechanism of the Data Sharer's environment; or

(v) use the technical environment of the Data Sharer to obtain access to data other than the Data covered by this Contract or in different conditions as this Contract sets out.

4.4 Security measures

4.4.1 Each Party will ensure the confidentiality, integrity and availability of the Data by implementing the appropriate security measures described in **Appendix 4** when making the Data available under access arrangements under 4.2.1.

4.4.2 If changes in the Data or their environment may affect the security of the Data, the Data Sharer and the Data Recipient agree to evaluate the security measures (specify: regularly/upon request

of the other party/upon special events), and to negotiate in good faith upon any necessary adaptation.

4.4.3 Each Party shall provide upon request to the other Party detailed information on implementation measures taken in accordance with this clause 4.4 and Appendix 4.

4.4.4 Each Party will report to the other Party any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Data within 24 hours of discovery.

4.4.5 [OPTION] [The Data Sharer reserves the right to conduct periodic audits or request documentation to verify compliance with security requirements imposed upon the Data Recipient.]

4.4.6 (if applicable) The Data Sharer undertakes not to keep any information on the Data Recipient's access to the Data requested beyond what is necessary for:

(a) the access to the Data;

(b) (if applicable) the security and the maintenance of the data infrastructure; and

(c) compliance with legal obligations to which the Data Sharer is subject.

The Data Sharer will inform the Data Recipient about the information kept by the Data Sharer in accordance with applicable laws or if requested by the Data Recipient.

4.5 Duty to re-negotiate, feedback loops and unilateral changes

4.5.1 If the Data are made available in conformity with the contractual arrangements concerning data characteristics, access procedures or necessary means and information to access and use the Data, and if it appears that the agreed contractual arrangements are insufficient to access and use the Data as agreed in this Contract, the Parties undertake to enter into negotiations in good faith and adapt the contractual arrangements.

4.5.2 If the Data Recipient identifies an incident related to clause 2 on the Data covered by the Contract or to clause 4.1 and 4.2. on the Data characteristics and access arrangements, and if the Data Recipient notifies the Data Sharer with a detailed description of the incident, the Data Sharer and the Data Recipient must cooperate in good faith to identify the reason for the incident. If the incident was caused by the Data Sharer failing to comply with their obligations, they must remedy the breach without undue delay. If the Data Sharer does not do so, it is considered to be a fundamental breach and the Data Recipient may invoke clause 10 of this Contract on remedies for breach of contract.

4.5.3 If any of the contractual arrangements agreed in accordance with clauses 4.1 to 4.2 are impossible or excessively onerous to achieve because of an exceptional change of circumstances occurring after conclusion of the Contract, the Data Sharer must provide the Data Recipient with a detailed description of this situation and the Parties will enter into negotiations in good faith and adapt the contractual arrangements. In particular, each Party must provide to the other

sufficient information to assess, discuss and resolve the particular situation. This clause does not affect the right of the Data Recipient to invoke remedies in accordance with clause 10.

4.5.4 The Data Sharer may, in good faith, unilaterally change details regarding the contractual arrangements for the data and access arrangements, if this is objectively justified by the normal conduct of business of the Data Sharer, for example by a technical modification due to an immediate security vulnerability in the line of products or related services offered by the Data Holder or by a change in the Data Sharer's infrastructure. Any change must meet the fundamental requirements of clauses 4.1 and 4.2.

4.5.5 The Data Sharer must give notice of the change to the Data Recipient at least (*indicate a reasonable period of time*) before the change takes effect.

A shorter notice period may suffice:

(a) where the change does not negatively affect access to and use of the Data by the Data Recipient; or

(b) where such notice would be impossible or unreasonable in the circumstances, such as where immediate changes are required because of a security vulnerability that has just been detected.

Where the change negatively impacts access to and use of the Data by the Data Recipient, the Parties undertake to work together to mitigate such impact. The Data Recipient may in any case terminate the (relevant part of the) Contract without any compensation being due to the Data Sharer, this notwithstanding any other rights or remedies the Data Recipient may have.

5. Use of the Data and sharing with third parties

5.1 Use of Data

5.1.1 Authorised purposes (Please select only one option)

[RESTRICTIVE OPTION] [The Data Recipient may process the Data only for the purposes of: *(specify authorised purposes)* ('Authorised Purposes')].

or

[BROAD OPTION for non-personal data only] [The Data Recipient may process the Data for any lawful purpose ('Authorised Purposes') [OPTION] [other than (specify, e.g. use the data it receives to derive insights about the economic situation, assets and production methods of or use by the Data Sharer)].]

(*If applicable, where the Data contain product or related service data and the Data Sharer under this Contract has gained access to it in accordance with Article 4 or 5 of the Data Act in their role as a user or a Data Recipient*) In any case, the Data Recipient must not use the data it receives to develop a product that competes with the product from which the Data originate.

When agreeing on the Authorised Purposes, the Parties should into account any restrictions arising from applicable law or their contractual commitment towards third parties. For instance, if the Data

are product data as defined in the Data Act and if the Data Sharer is a user of the product or a Data Recipient within the meaning of the Data Act, they should comply with the prohibition on developing a competing product provided for in Articles 4(10) and 6(2)(e) of the Data Act. If the Data Sharer is a user of this kind and agreed to specific restrictions on their legal rights under the Data Act with the Data Holder, this Contract should comply with such restrictions.

5.1.2 Authorised operations on the Data (Please select only one option)

[RESTRICTIVE OPTION] [The Data Recipient may only implement the following operations on the Data: (*specify authorised operations, e.g. access and copy Data to create aggregated statistics in relation to the Authorised purposes*) ('Authorised Operations').]

or

[BROAD OPTION for non-personal data only] [The Data Recipient may implement on the Data any lawful operation ('Authorised Operations') [OPTION] [other than (*specify, e.g. host or otherwise transfer or make accessible Data outside of the European Union, or attempt to identify data subjects*)]

(*If applicable, where the Data contains product or related service data and the Data Sharer under this Contract has gained access to them in accordance with Article 4 or 5 of Regulation (EU) 2023/2854 in their role as a user or a Data Recipient*) In any case, the Data Recipient must not use the data they receive in a manner that adversely impacts the security of the Product or any Related Service.]

5.1.3 Furthermore, the Data Recipient undertakes not to engage in the following conduct for the purposes of obtaining Data:

(a) provide false information to the Data Sharer;

(b) deploy deceptive or coercive means;

(c) abuse gaps or exploit any vulnerabilities in the technical infrastructure of the Data Sharer designed to protect the Data.

5.1.4 The right to use the Data in accordance with this clause is granted to the Data Recipient *(specify: in perpetuity/for the duration of the Contract/for a duration of (specify))*.

5.1.5 (If applicable in case of retrieval of the Data by/transfer of Data to the Data Recipient and if the Parties agree on a limitation in time of the use of the Data) Upon termination or expiration of their right to use the Data, the Data Recipient undertakes to permanently delete the Data (including any copy or backup) and to ensure that any third parties to whom the Data have been disclosed permanently delete such Data. The Data Recipient shall, without undue delay, provide written certification of such deletion upon the Data Sharer's request.

5.2 Sharing of Data with third parties

5.2.1 The Data Recipient shall not share or transfer any Data to any third party, whether in identified, anonymised or pseudonymised or aggregate form [OPTION] [, except that the Data Recipient may share the Data solely for the following use of the Data: *(specify)*. The third party shall not

share or transfer any Data further, [OPTION] [except for the following use of the Data: *(specify)*]].

5.2.2 (if applicable, where the Data contains product or related service data and the Data Sharer under this Contract has gained access to it in accordance with Article 4 or 5 of the Data Act in their role as a user or as a Data Recipient) The Data Recipient must not make the Data they receive available to an undertaking designated as a gatekeeper under Article 3 of Regulation (EU) 2022/1925 (Digital Markets Act).

5.2.3 Where the Data Recipient is permitted to make Data available to a third party on the basis of this contract, the Data Recipient must:

(a) [OPTION] [inform the Data Sharer of the fact that Data will be made available to a third party, specify the Data in question, and provide the Data Sharer with the identity and contact details of the third party;]

(b) take appropriate contractual, technical and organisational measures to make sure that the third party complies with the same or substantially equivalent obligations that arise for the Data Recipient from this Contract. This includes in particular the Data Recipient's obligations to:

(i) make sure that the third party applies at least the same security measures and obligations agreed by the Data Recipient under the clause 'Security measures'; and

(ii) make sure that the third party uses the data exclusively in a way compatible with clause 5.1 on the use of the Data; and

(iii) [OPTION] [make sure that the Data Sharer has at least the same remedies against the third party for unauthorised use or disclosure of Data as against the Data Recipient under this Contract; and]

(iv) *(applicable if the third party is entitled to make the Data available to other parties in accordance with clause 5.2.1)* [require the third party to ensure that all subsequent third parties receiving the Data comply with the obligations set out in this Contract].

5.2.4 Notwithstanding clauses 5.2.1 to 5.2.3, the Data Recipient may use processing services, e.g. cloud computing services (including infrastructure as a service, platform as a service and software as a service), hosting services, or similar services to use the Data as agreed under clauses 5.1.1 and 5.2.1, for their own account and under their own responsibility. The third

parties may also use such services to use the Data as agreed under clause 5.2.1, for their own account and under their own responsibility.

6. (if the data are protected as trade secrets) Trade Secrets

About trade secrets:

Trade secrets are confidential information that confers a competitive advantage on a company.

According to Article 2(1) of Directive (EU) 2016/943, the term 'trade secret' means information which meets three requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; and (c) it has been subject to reasonable steps in the circumstances, by the person lawfully in control of the information, to keep it secret.

'Trade Secret Holder' means any natural or legal person lawfully controlling such a trade secret.

When it comes to data, the Data Sharer is eligible for trade secret protection especially when digital information covers:

- technical information (product technology, R&D data, process know-how, unpatented technologies…);
- commercial information (market strategies, financial information…).

Thus, regarding digital information, the Data Sharer needs to identify a potential trade secret. For more information on trade secrets in the digital sector, see the WIPO Guide to Trade Secrets and Innovation:

https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html

Limited access for others, encryption or NDAs would be methods of keeping data secret, thus enabling trade secret protection to take place.

How to deal with trade secrets?

If the Data Sharer identifies certain trade secrets as being part of data sharing under the Contract, it is not obliged to share such data unlike under Article 4(6) and Article 5(9) of the Data Act.

Should the Data Sharer decide to share such data, it may set and agree requirements with the Data Recipient as a condition for sharing data protected as trade secrets, such as taking certain additional technical and organisational measures in order to preserve confidentiality. The Data Sharer and the Data Recipient should, in **Appendix 2** as part of the Contract, include all the details on the Data which are protected as trade secrets.

6.1 Applicability of trade secret arrangements

6.1.1 The protective measures as well as the related rights agreed below apply exclusively to data or metadata included in the Data to be made available by the Data Sharer to the Data Recipient, which are protected as trade secrets (as defined in Article 2(1) of the Trade Secrets Directive

(EU) 2016/943), held by the Data Holder or another Trade Secret Holder (as defined in Article 2(2) of that Directive).

6.1.2 The Data protected as trade secrets and the identity of the Trade Secret Holder are set out in **Appendix 2**.

6.1.3 The obligations set out in clauses 6.2 and 6.3 remain in effect after any termination of the Contract, unless otherwise agreed by the Parties.

6.2 Protective measures to be taken by the Data Recipient

The Data Recipient shall apply the protective measures as set out in **Appendix 4** (hereinafter: 'Data Recipient's Protection Measures').

Parties should, in **Appendix 4**, include all the details of the protection measures. Measures may be both of a technical (e.g. encryption, firewalls, split storage, etc.) and of an organisational nature (e.g. internal governance, appropriate identity management and access controls, involvement of a trusted third party).

As the measures need to be proportionate, their content will vary, depending on the nature of the trade secret. The measures will also depend on whether (i) access is to be provided where the Data are stored or (ii) the data are to be fully transferred to the Data Recipient. In the former case, the Data Holder has a higher degree of control and can apply part of the protective measures themself, whereas the Data Recipient may have a lower level of use for the Data. In any case, both Parties will need to focus on achieving the intended effects of this Contract.

6.3 Protective measures taken by the Trade Secret Holder

6.3.1 The Data Sharer may apply the measures agreed in Appendix 4 to preserve the confidentiality of Data protected as trade secrets (hereinafter: 'Data Sharer's Protection Measures').

6.3.2 The Data Sharer may also add unilaterally appropriate technical and organisational protection measures, if they do not negatively affect access to and use of the Data by the Data Recipient under this Contract.

6.3.3 The Data Recipient undertakes not to alter or remove the Data Sharer's Protection Measures nor the measures taken in accordance with 6.3.2, unless otherwise agreed upon by the Parties.

6.4 Third party identified Trade Secrets Holders

6.4.1 The Data Sharer declares to the Data Recipient that they have all relevant rights from any third party trade secrets holders to enter into this Contract regarding the Data protected as trade secrets.

6.4.2 The Data Recipient's Protection Measures and the Data Sharer's Protection Measures reflect the contractual commitments of the Data Sharer towards the initial Data Holder. Should such commitments from the Data Sharer towards the initial Data Holder evolve, the Data Recipient

commits to comply with any new measures agreed upon between the Data Sharer and the initial Data Holder.

7. Intellectual Property Rights

'Intellectual Property Rights' means copyright (including author's rights ('droit d'auteur'), rights in computer software and other neighbouring rights), rights in designs (including registered designs and design rights), trademarks, service marks, trade or business names, brand names, domain names and URLs, rights in trade secrets, know-how and confidential and undisclosed information (such as inventions, whether patentable or not), rights in logos and patents, sui generis rights in databases and any similar rights recognised under applicable law.

The data within the scope of this Contract and the allowed use by the Data Recipient must be regulated by this Contract to protect intellectual property rights of the Data Sharer, third parties or newly emerging IP rights of the Data Recipient. Regarding data sharing, the most important IP rights which must be taken into consideration when concluding a contract are the sui generis right of the Database Directive and copyright.

Sui generis right:

According to Article 43 of the Data Act, *The sui generis right provided for in Article 7 of Directive 96/9/EC shall not apply when data is obtained from or generated by a connected product or related service falling within the scope of this Regulation, in particular in relation to Articles 4 and 5 thereof*'. However, '*That does not affect the possible application of the sui generis right under Article 7 of Directive 96/9/EC to databases containing data falling outside the scope of this Regulation, provided that the requirements for protection pursuant to paragraph 1 of that Article are fulfilled*' (Recital (112)).

The *sui generis* right of the Database Directive protects the maker of the database as this is the person who made substantial investments in terms of quality or quantity for the acquisition, verification or presentation of its content. The maker can prohibit extraction and reutilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. Individual works or data elements within the database, if they are original, might be separately protected by copyright, though this protection is distinct from the protection provided by the Database Directive.

Copyright:

Copyright is a form of intellectual property protection granted by law to the creators of original works of authorship. This protection covers a wide range of works, including potentially the architecture of a database. Please note: Copyright protection has not been fully harmonised and may therefore vary between Member States.

Patents:

Data sharing and use of the data can lead to inventions as they inspire new ideas, optimise existing technologies, and accelerate the development of innovative solutions. Inventions of a technical character that are new and involve inventive steps that can be used in an industry are patentable. The Parties should therefore regulate inventions and who is entitled to use these patentable results.

7.1 Prior Intellectual Property Rights

7.1.1 Unless expressly provided otherwise in the Contract, each Party retains ownership of any Intellectual Property Rights owned by the Parties, or licensed to them by third parties, before or

completely independently from the performance of the Contract, including any amendments and/or improvement thereto ('Pre-Existing Elements'). In no circumstances may the Contract be deemed to grant either Party any Intellectual Property Right in the other Party's Pre-Existing Elements except as otherwise expressly provided in the Contract.

7.1.2 *(applicable if the Data are covered by intellectual property rights)* Subject to the payment of the renumeration(e.g. licence fees) under this Contract, the Data Sharer hereby grants the Data Recipient for the term of the Contract a license covering the following characteristics: *(please specify, e.g. worldwide, non-exclusive, non-transferable* including the right to (*please specify, e.g. use, copy, modify, enhance, maintain*) the Data that would be covered by an Intellectual Property Right solely to the extent necessary under the Contract. A sublicence to the Data Recipient's subcontractors is authorised only for the purposes of the subcontracting and to the extent they are not incompatible with the provisions of this Contract.

7.2 Intellectual Property Rights on the Results

7.2.1 Should the use of the Data by the Data Recipient under this Contract generate tangible work products which are capable of being protected by Intellectual Property Rights ('Results'), it is hereby agreed that: (select only one option)

7.2.2 [OPTION 1] the Data Recipient shall become the sole owner of any and all Intellectual Property Rights relating to the Results; only the Data Recipient may, at their discretion, register for or obtain any such intellectual property title;

7.2.3 [OPTION 2] the Parties will be jointly and equally entitled to the Intellectual Property Rights on the Results and shall enter into a separate contract describing the modalities of the exercise of such rights;

7.2.4 [OPTION 3] the Data Recipient agrees to assign, to the extent necessary, to the Data Sharer the full legal and beneficial ownership of, and all Intellectual Property Rights in, the Results on an exclusive basis for a consideration to be further agreed between the Parties, worldwide, for the entire duration of Intellectual Property Rights.

7.2.5 Moreover, the Parties agree that further licensing on the Results shall be granted as follows (select as many options as appropriate):

[OPTION 1] *(specify the party which does not own IPR on the Results)* hereby grants to the *(specify the owner of the IPR on the Results)*, for the duration of protection of Intellectual Property Rights, a fully paid worldwide, non-exclusive, non-transferable licence to use, copy, modify, enhance and maintain its Pre-Existing Elements solely to the extent necessary to perform its rights on the Results under this clause.

[OPTION 2] (*specify the owner of the IPR on the Results*) hereby grants to the (*specify the Party which does not own IPR on the results*), for the duration of protection of Intellectual Property Rights, a fully paid worldwide, non-exclusive, non-transferable licence to use, copy, modify, enhance and maintain the Results solely for the following purposes: (*please fill in as applicable*).

8. Renumeration for provision of data access

The Parties may, in the Contract itself or in a separate appendix, determine details on renumeration including costs for setting up the API (used for the sharing of the Data) or other costs associated with facilitating the sharing of Data, including any royalties or licence fees, as the case may be. The Parties should agree, at least, on the following: amount of renumeration due, and the relevant currency; time when renumeration is due; and payment procedures.

They may agree on further renumeration, where applicable, for additional services, which will be subject to an additional fee.

The Parties agree that the Data Recipient will renumerate the Data Sharer as follows: *(fill in as appropriate)*

Parties should agree, at least, on the following: amount of renumeration due, and the relevant currency; time when payment is due; and payment procedures.

9. Date of application, duration of the Contract and termination

9.1 Date of application and duration

9.1.1 This Contract [OPTION 1] [takes immediate effect] [OPTION 2] [takes effect from *(specify date)*].

9.1.2 [OPTION] [This Contract is concluded for [OPTION 1] [an indeterminate period] [OPTION 2] [a fixed period of (*specify)*], subject to any grounds for expiry or termination under this Contract.]

9.1.3 [OPTION] [The Data Sharer must start making the Data available to the Data Recipient [OPTION 1] without undue delay after the Contract has come into effect. [OPTION 2] on (*insert date and, where applicable, further details as to timing*).]

If the request is for a one-off supply of data, it is sufficient to agree on the date of application in clause 9.1.1. If the request is for a continuous supply of data, the Parties will need to agree on the duration of the Contract and choose either the first or second option in clause 9.1.2.

9.2 Termination for convenience

9.2.1 The Data Recipient may terminate the Contract at any time during the Contract period by giving the Data Sharer a notice of *(insert period)*.

9.2.2 [OPTION] Where the Data Recipient terminates the Contract under clause 9.3.1. before *(insert point in time or minimum contract period)*, they must compensate the Data Sharer for the costs

incurred by the Data Sharer for making the data available, including, where applicable, providing any additional support, as follows: *(specify)*

> There may be cases where the Data Sharer incurs expenses when making the Data available to the Data Recipient, such as by adapting their digital infrastructure, trusting that these expenses will be amortised over time.
>
> In this case, the Data Sharer may want to make sure that they receive compensation from the Data Recipient.

9.3 Effects of expiry or termination

9.3.1 Expiry of the Contract period or termination of this Contract releases both Parties from their obligation to effect and to receive future performance but does not affect the rights and liabilities that have accrued up to the time of termination.

Expiry or termination does not affect any provision in this Contract for settling disputes under clause 11.6 or any other provision which is to operate even after the Contract has come to an end.

9.3.2 [OPTION 1] [The Data Sharer must take appropriate exit support measures as the Data Recipient may reasonably expect.] [OPTION 2] The Data Sharer must take the following exit support measures: (specify).]

> Parties may consider whether the Data Recipient requires any exit support measures.
>
> This will be relevant, for example, if the Data Recipient was allowed to extract Data from a medium controlled by the Data Sharer but had not yet extracted the Data because they did not expect the Contract to be terminated.

10. Remedies for breach of contract

10.1 Cases of non-performance

10.1.1 A non-performance of an obligation is fundamental if:

(a) the non-performance substantially deprives the other Party of what it was entitled to expect under this Contract, unless the non-performing Party did not foresee and could not reasonably have foreseen that result; or

(b) it is clear from the circumstances that the non-performing Party's future performance cannot be relied upon.

10.1.2 A Party's non-performance is excused if it is due to an impediment beyond its control and if that Party could not reasonably have been expected to take the impediment into account at the

time of the conclusion of this Contract, or to have avoided or overcome the impediment or its consequences.

Where the impediment is only temporary, the excusing of the Party's non-performance has effect for the period during which the impediment exists. However, if the delay amounts to a fundamental non-performance, the other Party may treat it as such.

The non-performing Party must ensure that notice of the impediment and of its effect on its ability to perform is received by the other Party without undue delay after the non-performing Party knew or could reasonably be expected to have become aware of these circumstances. The other Party is entitled to damages for economic damage resulting from the non-receipt of such notice.

10.2 Remedies for breach

10.2.1 In the case of a non-performance by a Party, the other Party shall have the remedies listed in the following clauses, without prejudice to any remedies available under applicable law.

10.2.2 Remedies which are not incompatible may be cumulated.

10.2.3 A Party may not resort to a remedy to the extent that they cause the other Party's non-performance, such as where a shortcoming in its own data infrastructure did not allow the other Party to duly perform its obligations. A Party may also not rely on a claim for damages suffered to the extent that it could have reduced the damage by taking reasonable steps.

10.2.4 The aggrieved Party can:

(a) terminate this Contract with immediate effect without penalty, by giving notice to the other Party, if:

(i) the other Party's non-performance is a fundamental non-performance; or

(ii) in the case of a non-performance which is not fundamental, the aggrieved Party has given notice requiring the non-performance to be remedied without undue delay and the other Party has not done so.

(b) claim damages for economic damage caused to them by the other Party's non-performance which is not excused under clause 10.1.2; the non-performing Party is liable only for damage which it foresaw or could be reasonably expected to have foreseen at the time of conclusion of this Contract as a likely result of its non-performance, unless the non-performance was intentional or grossly negligent;

(c) request that the non-performing Party complies, without undue delay, with its obligations under this Contract, unless it would be unlawful or impossible or specific performance would cause the non-performing Party costs which are disproportionate to the benefit the other Party would obtain.

10.2.5 [OPTION] [Where a Party fails to perform its obligations under this Contract it shall, in any case, pay the penalties set out in detail in Appendix 5, which the Parties deem damages within the meaning of clause 10.2.4(b). The non-performing Party has the right to request that the

penalty is reduced to a reasonable amount where they can prove that the penalty is grossly excessive in relation to the damage resulting from the non-performance.]

11. General provisions

11.1 Confidentiality

11.1.1 The following information must be considered confidential:

(a) information referring to the trade secrets, financial situation or any other aspect regarding the operations of the other Party unless the other Party has made this information public;

(b) information setting out the basis for the calculation of the reasonable compensation;

(c) information referring to any third party, unless they have already made this information public.

11.1.2 Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 11.1.1. and not to disclose or make available such information to any third party, unless:

(a) one of the Parties is under a legal obligation to disclose or make the relevant information available; or

(b) it is necessary for one of the Parties to disclose or make the relevant information available to fulfil their obligations under this Contract; or

(c) one of the parties has obtained the prior consent from the other Party or the party providing the confidential information or affected by its disclosure.

11.1.3 These confidentiality obligations remain applicable after the termination of the Contract for a period of *(specify the period)*.

11.1.4 These confidentiality obligations do not remove any more stringent obligations under (i) Regulation (EU) 2016/679 (GDPR), (ii) the provisions implementing Directive 2002/58/EC or Directive (EU) 2016/943 or (iii) any other EU or Member State law.

11.2 Means of communication

Any notification or other communication required or permitted to be given under this Contract must be in writing and may be delivered by hand, sent by prepaid post, or transmitted by electronic means, including email, provided that the sender retains proof of sending to the addresses listed below:

Party	**Contact Person**	**Email**	**Phone**	**Address**
User	[Name]/[Position]	[Email]	[Phone]	[Address]
Data Recipient	[Name]/[Position	[Email]	[Phone]	[Address]

Any such notice or communication will be deemed to have been received:

(a) if delivered by hand, on the date of delivery;
(b) if sent by prepaid post, on the third business day after posting;
(c) if sent by electronic means, on the date of transmission, provided that no error message indicating failure to deliver has been received by the sender.

11.3 Entire Contract, amendments and severability

11.3.1 This Contract (together with its appendices referred to in the Contract) constitutes the entire Contract between the Parties with respect to the subject of this Contract and supersedes all prior contracts or agreements and understandings between the Parties, oral or written, as regards the subject of this Contract.

11.3.2 Any amendment to this Contract will be valid only if agreed to by the Parties in writing, including in any electronic form.

11.3.3 If any provision of this Contract is found to be void, invalid, voidable or unenforceable for whatever reason, and if this provision is severable from the remaining terms of the Contract, these remaining provisions will be unaffected by this and will continue to be valid and enforceable, unless the provision is not severable from the remaining provisions of this Contract. Any resulting gaps or ambiguities in this Contract must be dealt with in accordance with clause 11.5.

11.4 Applicable law

This contact is governed by the law of *(specify state)*.

11.5 Interpretation

11.5.1 Any provision in this Contract must be interpreted so as to comply with Union law or national legislation adopted in accordance with Union law, as well as any applicable national law that is compatible with Union law and cannot be derogated from by agreement.

11.5.2 If any gap or ambiguity in this Contract cannot be resolved in the way referred to in clause 11.5.1, this Contract must be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 11.4).

11.6 Dispute settlement

11.6.1 The Parties agree to use their best efforts to dissolve disputes amicably and, before bringing a case before a court or tribunal, to submit their dispute to [insert name and contact details of a particular dispute settlement body].

11.6.2 [OPTION] [The courts of (*specify state*) will have exclusive jurisdiction to hear the case concerning this Contract.]

Appendix 1 contains a description of the Data

[to be drafted by the Parties]

Appendix 2 contains further details regarding Data covered by a regime requiring specific measures

[to be drafted by the Parties]

Appendix 3 contains details on Personal Data and respective obligations of the Parties

[to be drafted by the Parties]

Appendix 4 contains applicable security measures for the sharing of Data

[to be drafted by the Parties]

[OPTION] Appendix 5 contains details on penalties

[to be drafted by the Parties]

Standard Contractual Clauses

ANNEX VI: STANDARD CONTRACTUAL CLAUSES
on Switching and Exit

The primary goals of Regulation (EU) 2023/2854 (referred hereto as the Data Act)'s provisions on cloud switching include enabling Customers of Data Processing Services (cloud computing and edge services) to: (i) switch between Providers offering the same service type, (ii) switch to an on-premises ICT infrastructure; or (iii) make use of multiple services from different providers simultaneously. Therefore, the Data Act specifies the rights and obligations of Providers and Customers with regard to this process. In this context, Customers should also assess their objectives related to switching and, in particular, specific needs, additional expenditures or timing. Both the Source Provider, the Customer and the Destination Provider must cooperate in good faith to make the switching process effective, enable the timely transfer of Data and maintain the continuity of the Data Processing Services (Article 27 of the Data Act).

These SCCs translate the new rights and obligations introduced by the Data Act as regards the switching and exit process into contractual terms. The Data Act requires Providers to provide Customers with a written contract setting out the arrangements of the switching process. The Contract must also specify timelines for switching (maximum transitional period of 30 days) and details of any costs involved (including early termination penalties, standard service fees (Article 29(4) of the Data Act and Egress charges). There are also obligations in relation to the switching process itself that should be specified in the contract: providing reasonable assistance to the Customer (and any third parties authorised by the Customer), maintaining business continuity and ensuring a high level of security throughout the switching process.

Switching charges

As per Article 29 of the Data Act, a Provider can maintain switching charges up to 12 January 2027, but these cannot exceed costs incurred by the Provider that are directly linked to the switching process. For switching after 12 January 2027, the Provider is not allowed to impose switching charges. The switching charges include egress charges and other costs for actions which the provider is required to carry out as part of the switching process. This includes, for instance, costs for the use of automated switching tools or testing tools, where these are used by the provider to comply with its obligations under the Data Act.

Where a Data Processing Service is being used in parallel with another Data Processing Service, the Providers may – even after 12 January 2027 – continue to pass on costs incurred for Data Egress to the Customer (Article 34 of the Data Act).

Where the Data Act defines "switching charges" as charges „*imposed by a provider of data processing services on a customer for the actions mandated by this Regulation for switching to the system of a different provider or to on-premises ICT infrastructure* […]", Article 25 (2)(a)(i) of the Data Act also specifies that the provider must "*provide reasonable assistance to the customer and third parties authorised by the customer in the switching process*". Any charges related to the provision of such "reasonable assistance" should be withdrawn over time as mentioned in Article 29.

The Data Act specifies cases where a standard approach is not possible:

- Article 29(5) "*Where relevant, providers of data processing services shall provide information to a customer on data processing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or Service architecture*,"
- and Article 29 (6): *"Where applicable, providers ...shall make the information ...publicly available*..".

Other standard contractual clauses recommended by the Commission can be found attached hereto and they cover specific topics other than switching and exit. The Parties are encouraged to consider using those other clauses, too, as they were developed to be coherent and reinforce each other.

Specific regime

It is worth noting that Article 31 of the Data Act provides for certain exceptions to certain obligations related to the SCCs Switching & Exit. For instance, a specific regime applies to switching Data Processing Services if:

(a) most of the main features of the Data Processing Service have been custom-built for the specific needs of an individual customer OR all components have been developed for the purposes of an individual customer; and
(b) those Data Processing Services are not offered at broad commercial scale via the Provider's service catalogue; and
(c) where the Provider has duly informed the Customer that the obligations on switching do not apply to this particular service.

Depending on the particular exception, certain legal obligations may not apply. However, it is up to the Customer and the Provider to agree whether to include these in their Agreement. While these standard contractual clauses were not drafted to cover such situations, they can still serve as an inspiration for the parties to an Agreement/contract concerning such services.

The Provider should inform prospective customers, well before the conclusion of an Agreement, about specific Services to which the specific regime laid down in the Article 31 of the Data Act applies.

Nothing prevents the Provider from eventually deploying such services at scale, in which case that Provider would have to comply with all obligations for switching laid down in the Data Act.

Approaches to switching

An increasing number of Providers offer self-service switching tools for both data ingress, when Customers start using a service, and Data Egress when Customers stop using a service and switch either to an on-premises system or to a new (Destination) Provider. For some Data Processing Services, there may not be such tools, or they may not enable complete switching.

Two approaches to planning and executing the switching process are provided for in these SCCs:

(a) switching based on the switching and exit plan (Option A); and
(b) switching with the use of automated tools (Option B).

These options may be combined. For example, in **Appendix 1** "Switching and Exit Plan" the Parties may also envisage the use of automated tools which may apply for some service types or some Data.

Under both approaches, Providers are obliged to remove obstacles to effective switching as laid down in Regulation (EU) 2023/2854 whereby the Providers "*shall provide the customer with: information on available procedures for switching and porting to the data processing service, including information on available switching and porting methods and formats as well as restrictions and technical limitations which are known to the provider of data processing services*" (Article 26(a)); and "*the source provider of data processing services shall facilitate the switching process by providing capabilities, adequate information, documentation, technical support and, where appropriate, the necessary tools*" (Article 30).

It is also important to note that the Provider is not expected to share or list any Data specific to the internal functioning of the Provider's Data Processing Service where a risk of breach of the Provider's trade secrets exists. As per the contractual obligations laid down in Article 25(2)(f), the Provider is required only to provide an exhaustive specification of categories of such Data.

Are the SCCs applicable to all models of cloud services (e.g. to IaaS, PaaS or SaaS contracts)?

These SCCs are applicable to all types of models of cloud service contracts, where the cloud service in question meets the definition of a Data Processing Service laid down in Article 2(8). According to this article, a Data Processing Service is "a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction". The provisions of the Data Act thus apply to service types which display the characteristics listed in the definition of data processing services:

- they enable access to computing resources, including networks, servers, storage, applications, and services;
- they enable on-demand network access, meaning that a customer can unilaterally provision these computing resources which are available over the network and through standard mechanisms, for example via mobile phones, laptops, or work stations;
- they can be rapidly provisioned and released with minimal management effort or service provider interaction, which implies that the unilateral provision can be done without significant intervention from the service provider and can be deployed quickly, allowing organisations to start using the resources almost immediately;
- they are elastic and can be rapidly provisioned, meaning that the solutions can easily scale to accommodate changing needs and that users can upgrade or downgrade demand based on their requirements.

A Provider whose service offering displays these characteristics must comply with the provisions of the Data Act to enable switching between Data Processing Services. This includes, for example, bringing service contracts into line with Article 25, reducing and removing switching and egress charges pursuant to Article 29, and complying with the technical aspects of switching defined in Article 30. However, not all requirements placed on data processing services under Chapter VI of the Data Act apply to SaaS. Notably, the concept of functional equivalence laid down in Article 30(1) only applies to providers of IaaS, whereas Articles 30(1) and 30(2) apply to providers of PaaS and SaaS. These latter two provisions require providers of PaaS and SaaS to make open interfaces available and comply with open interoperability specifications and harmonized standards published in an EU repository.

Article 30 of the Data Act differentiates between:

1. IaaS defined as "*data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements*."

   and

2. other types of cloud services.

Furthermore, recital 81 of the Data Act specifies that the generic concept of "data processing services" covers a substantial number of services with a very broad range of different purposes, functionalities and technical set-ups and they are commonly understood to fall into one or more of the three Data Processing Service delivery models i.e. IaaS, PaaS and SaaS.

Capacities of the Parties

Article 24 of the Data Act clarifies that "*the responsibilities of providers of data processing services laid down in Articles 23, 25, 29, 30 and 34 shall apply only to the services, contracts or commercial practices provided by the source provider of data processing services."*

Among other elements, knowledge of the structure of the Data and the relationship between Data is required to define the sequence of operations for exporting the Exportable Data. The list below, therefore, provides general guidance to the Parties to help their understanding of each other's capacity underpinning different parts of the switching process. However, the list is only indicative and there are important nuances that can differ between and within the service model categories below, depending on the particular Data Processing Service in question. Parties should pay close attention to such differences.

IaaS

- The Customer knows the structure of the database that they have defined. The IaaS Provider does not know the structure of the database. The IaaS Provider is able to give details regarding the porting methods and, where appropriate, the necessary tools.
- The Customer is able to define the sequence of operations, a time window and the required IT resources.
- The Provider is able to confirm the availability of the required IT resources during the time window.
- The Customer is able to initiate switching at the agreed time.
- The Customer is responsible for importing the Data in the destination environment and implementing it there.

PaaS

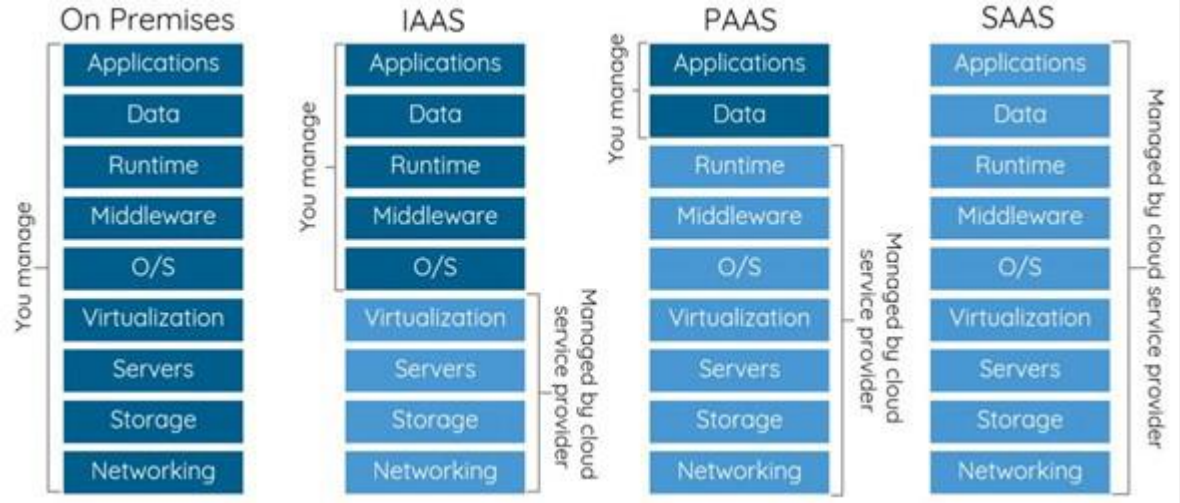
- The Customer knows the structure of the database that they have defined.
- The PaaS Provider also knows characteristics of the database because the Customer asked them to provide services such as space allocation, optimisation, reorganisation, and backups.
- The PaaS Provider has a practical experience of the procedures for operations such as backups. They know the resources required and the time which has elapsed. The PaaS Provider is able to give details regarding the porting methods and, where appropriate, the necessary tools and information about the timing and required IT resources.
- The Customer is able to define the sequence of operations, a time window (a period, such as a weekend, during which the Customer intends to make their systems unavailable for the users and no update occur so that the Data are frozen, and the Customer may carry out the switching) and the required IT resources.
- The Provider is able to confirm the availability of the required IT resources during the time window.
- The Customer initiates the switching at the agreed time.

SaaS

- The Customer does not know the structure of the database.
- The SaaS Provider knows the structure of the database that they have defined.
- The SaaS Provider knows the procedures and the time required for operations like backups, optimisations and reorganisations.
- In the case of installation of a new version of the SaaS software with a new version of the database structure, it is not unusual to have a full export from the old structure followed by a full import into

the new structure. This procedure gives the SaaS Provider a practical view of the procedure, resources and time required to export the Data.

- The SaaS Provider is able to give details regarding the porting methods and, where appropriate, the necessary tools,
- and information about the timing and required IT resources
- and propose the exporting methods and formats and the sequence of operations
- The Customer is responsible for importing the Data in the destination environment and might have requirements and remarks on the proposed sequence.
- The SaaS Provider and the Customer are able to agree on the sequence of operations, the time window and the required IT resources
- The Provider is able to confirm the availability of the required IT resources during the time window.
- Depending on the tool and the sequence agreed, the Provider or the Customer initiate the switching at the agreed time.
- The Customer is responsible for importing the Data into the destination environment.



Actions during the maximum notice period and transitional period

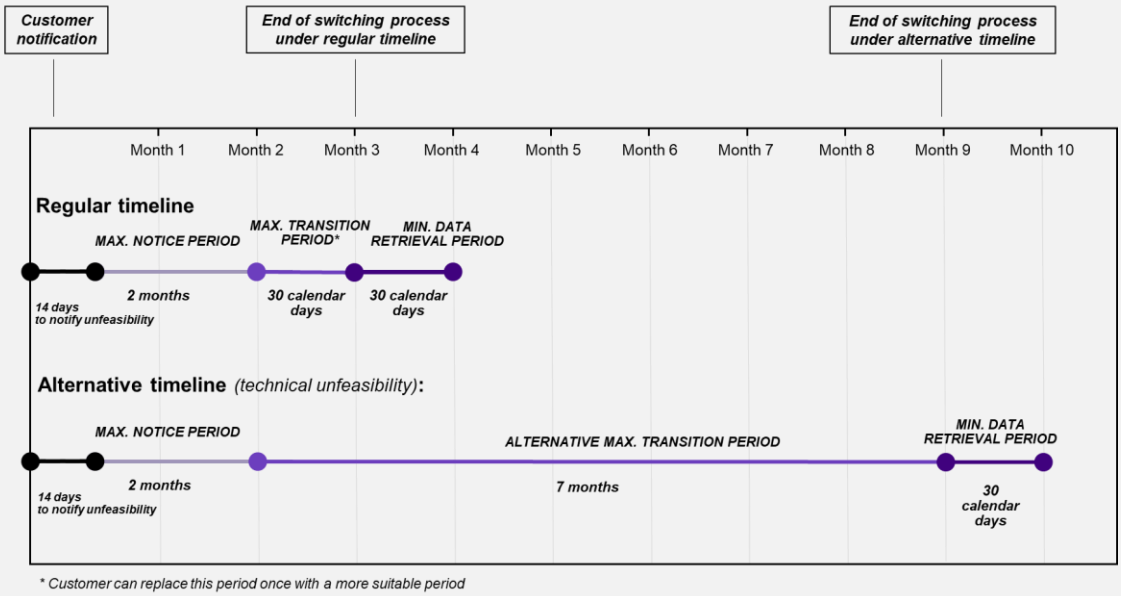
Initiating switching - Article 25(2)(d) of the Data Act requires contracts to provide for a maximum notice period for initiating the switching process, which must not exceed two months. This clause sets out what information the Provider should provide to the Customer in that period and what actions the Provider will take after initiating the switching process.

Transitional period - Article 25(2)(a) of the Data Act requires contracts to include provisions for the Customer to be able, on request, to switch to another Data Processing Service or transfer all Exportable Data to on-premises ICT infrastructure without undue delay, and in any event within no longer than the mandatory maximum transitional period of 30 calendar days starting with the end of the maximum notice period.

Article 25(2)(g) of the Data Act also requires the Contract to contain a minimum period for Data retrieval of at least 30 calendar days, starting after the termination of the transitional period agreed by the Parties.

Where the mandatory maximum 30-day transitional period for switching is technically unfeasible, the Provider must notify the Customer within 14 working days after the switching request has been made, explain the technical unfeasibility, and indicate an alternative transitional period, which may not exceed seven months

(Article 25(4)) of the Data Act). The Customer has the right to extend the mandatory maximum transitional period once, by a period that the Customer deems more appropriate (Article 25(5) of the Data Act).



The Data Processing Agreement is considered terminated upon completion of successful switching or at the end of the maximum notice period, if the Customer does not want to switch but to erase their Exportable Data and Digital Assets upon service termination. No termination notice from the Customer is needed, as the Agreement will terminate automatically. However, for the sake of legal certainty and to ensure that the interests of the Parties are protected, the Provider is obliged to notify the customer of the Contract termination (Article 25(2)(c) of the Data Act).

Option A: Switching and exit plan as an Annex to the Agreement

Before concluding the Contract, the Parties could consider designing a detailed plan for switching and exit. This can be useful, especially, in the case of complex Data Processing Services. The switching and exit plan included here gives the Parties a clear vision from the beginning of the contractual relationship regarding the switching process, including with regard to what types of information, Data and processes will need to be shared between the Parties in order to switch without any delay or impact on the Customer's services or business.

The template "switching and exit plan" in **Appendix 1** is only an example of such a plan that gives the Customer an idea of the questions which they will need to ask their Provider and of the structure of those discussions.

The division of responsibilities during the execution of the switching process is an example aligned, where relevant, with the rights and obligations enshrined in the Data Act. While respecting such rights and obligations, the Parties may agree to a different division or to the inclusion of further details.

For this reason, the plan is not the same as a standard contractual clause. One option is to keep it as a separate technical Annex to the Contract, which can be amended/updated by the Parties separately. Alternatively, the Parties may want to make the Annex part of the Contract itself.

This Annex could be a standard switching and exit plan proposed by the Provider and agreed by the Customer or it could be a customised switching and exit plan proposed by the Provider for the Customer.

The Parties could update the switching and exit plan during the Agreement as required by the evolution of the Data Processing Services and the Data covered by the Agreement, at periods agreed by the Parties. This update could also affect the agreed transitional period, for example, within the limits set by Regulation (EU) 2023/2854.

The switching and exit plan only applies when the Customer switches Providers, or to an on-premises ICT infrastructure, not if the Customer intends to have their Data deleted at the end of the notice period.

Option B: Self-service automated switching tools

Though the use of self-service automated switching tools is prevalent, it may come with certain challenges. A particular concern is, for example, that in the case of SaaS, some databases and their setups may not be migrated properly and/or completely, triggering the need for manual intervention by the Provider. If the Provider relies on such a self-service solution, the clauses in Option B allow the Customer to ensure that the Agreement contains sufficient information about the process and the tool. The elements included in Option A (Switching and exit plan as Annex to the Agreement) may serve as inspiration.

If a Provider employs switching tools to carry out the actions mandated by the Data Act for switching to the system of a different provider or to on-premises ICT infrastructure, the act of charging the Customer for the use of these switching tools would be considered to constitute a switching charge.

What if switching is unsuccessful? Clause 1.7 under Option A and clause 2.6 under option B cater for a situation in which switching is not successful by spelling out the steps that the Customer (and their Destination Provider) and the Source Provider will need to take, in good faith, to achieve successful switching and/or to prompt the option of Data erasure provided by the Data Act.

Example: The Source Provider proposes SaaS solution A and the Destination Provider proposes SaaS solution B. The Customer asks the Source Provider to help them switch to the Destination Provider via exporting and transferring their exportable Data to a specific server. The following scenarios could occur:

1. The Source Provider does not propose effective tools and procedures for exporting and transferring all Exportable Data to the specific server;
2. Data have been delivered to the specific server but the Customer or the Destination Provider are unable to upload the Data properly.

1. Option A: Switching and exit with a plan as an Annex to the Agreement

1.1 Information

1.1.1 The Parties confirm that the Provider has made available to the Customer in an Annex to the Agreement or on their website clear information about:

(a) their standard service fees and, where applicable, early termination penalties;

(b) the Switching Charges;

(c) services that involve highly complex or costly switching, or for which it is impossible to switch without significant interference in the Data, Digital Assets or service architecture, where relevant;

(d) specific services where the obligations on switching and exit do not apply, where relevant.

Article 31 of the Data Act lays down a specific regime for certain Data Processing Services. For custom-built or highly individualised services, certain switching obligations do not apply. The Parties need to agree on how such switching could take place (including the cost). For Data Processing Services provided as a non-production version for testing and evaluation purposes and for a limited period of time the obligations for switching do not apply. While these standard contractual clauses were not drafted to cover such situations, they can still serve as inspiration for the Parties to an Agreement concerning such services.

Under Article 30(6) of the Data Act, Providers will not be required to develop new technologies or services. Nor will they be required to disclose or transfer to a Customer or to a different Provider of Data Processing Services digital assets that: (i) are protected by intellectual property rights; or (ii) constitute a trade secret or (iii) compromise the Customer's or Provider's security and integrity of service.

1.2 Switching and exit

1.2.1 The Parties agree on a "switching and exit plan" (the "Plan"), using the form specified in Appendix 1, which forms an integral part of the Agreement and will be implemented by the Parties. The Plan contains:

(d) an exhaustive specification of all categories of Data and Digital Assets that can be transferred, including at a minimum all Exportable Data (Article 25(2)(e) of the Data Act);

(e) an exhaustive specification of categories of Data specific to the internal functioning of the Provider's Data Processing Service that will be exempted from the Exportable Data where there is a risk of breach of the Provider's trade secrets (Article 25(2)(f) of the Data Act).

(f) clear information concerning known risks to continuity in the provision of the functions or services on the part of the source Provider (Article 25(2)(a)(iii) of the Data Act).

(g) details regarding switching and exit assistance, including the porting methods and formats, and steps required to carry out the switching process;

(h) the name and contact details of the representative designated by the Customer and the Provider to carry out the Plan;

(i) an estimate of the time needed to export and transfer the Data and Digital Assets out of the source Provider's environment;

The Source Provider can support the Customer's switching process by providing an estimate of the time necessary to export and transport the Exportable Data outside its environment based on the time required to import the Data, the estimated volume, network capacity and previous experience or tests. Similarly, the Customer can estimate the time required to import and implement the Data into the destination environment. Both Parties should leverage such information to see if an alternative transitional period is needed.

(j) restrictions and technical limitations, including those arising from storage of Data outside the European Union;

(h) a description of the sequence of switching operations proposed by the Provider;

(i) a description of the testing method proposed by the Provider if tests are carried out.

1.2.2 The Provider provides the Customer with a reference to the on-line register with Data structures and formats, relevant standards and open interoperability specifications, where Exportable Data are available at [specify link to the location] (Article 26(b) of the Data Act).

1.2.3 If required by the Customer, the Provider must make available via adequate electronic means information explaining the relevant procedures to the Customer's designated personnel (or authorised third parties).

1.2.4 If requested by the Customer, the Provider will either arrange a test, or help the Customer to conduct a test, as agreed in Appendix 1, to check that the Plan works in practice for Exportable Data and Digital Assets. If problems appear during the test, the Parties will in good faith analyse the causes and agree on solutions.

1.2.5 The Provider and the Customer should update the Plan whenever necessary or at the Customer's request, backed up by a justification for the required changes.

1.3 Initiation of the switching process

1.3.1 The Customer initiates the switching by sending the Provider a switching notice as indicated in clause 1.10, observing the notice period of [P*arties to indicate the agreed notice period, which cannot exceed two months]*. If the Customer wishes to switch only with regard to certain services and the corresponding Data or Digital Assets, this must be specified in the switching notice. [OPTION] [The Costumer gives notice by using the form in **Appendix 3**].

> Subject to the terms of the Agreement, the Customer may choose to switch only a certain subset of services hosted by the source Provider. In that case, the switching obligations concern only such services and the corresponding Data and Digital Assets; for the rest, the previously agreed contractual terms still apply.

1.3.2 In the switching notice, the Customer informs the Provider whether they intend:

(a) to switch to a different Provider of Data Processing Services. In this case, the Customer provides necessary details of the Destination Provider (Article 25(3)(a) of the Data Act);
(b) to switch to an on-premises ICT infrastructure of the Customer (Article 25(3)(b) of the Data Act); or
(c) not to switch but only erase their Exportable Data and Digital Assets (Article 25(3)(c) of the Data Act).
(d) [OPTION] [The Costumer will give notice by using the form in **Appendix 4**]

1.3.3 The Provider confirms to the Customer the receipt of the switching notice not later than [within three working days] using the same means of communication as the one used by the Customer.

1.4 Transitional period

1.4.1 The Customer has the right to switch without undue delay within the maximum transitional period of 30 days. The Customer may agree with the Provider to the transitional period of (*Parties to indicate the agreed transitional period, which could be a maximum of 30 calendar days*) (Article 25.2(a) of the Data Act).

1.4.2 When the Provider cannot respect the [mandatory maximum] transitional period because this is not technically feasible, the Provider (Article 25(4) of the Data Act):

(a) notifies the Customer within 14 working days from [the date of the switching notice];

(b) indicates an alternative transitional period, which must not exceed seven (7) months from the date of the Customer's switching notice; and

(c) gives proper justification for the technical unfeasibility.

1.4.3 The Customer confirms receipt of the notice for an alternative transitional period [within three working days].

1.4.4 The Customer may extend the transitional period once, for a period they consider more appropriate for their own purpose, for no longer than [*specify the number of months*] (Article 25(5) of the Data Act). In that case, the Customer notifies the Provider as agreed in clause 1.11 of their intention before the end of the original transitional period and indicates the alternative transitional period. The Provider confirms the receipt of such extension notice [within three working days].

1.4.5 [OPTION] The Costumer gives notice for an alternative transitional period by using the form in Appendix 5.

1.5 Obligations of the Provider during the switching process

1.5.1 The Provider undertakes to provide reasonable assistance to the Customer and third parties authorised by the Customer in the switching process once the switching process starts and throughout it so that the Customer can switch within the transitional period. To this effect, the Provider must, in particular:

(a) provide capabilities, adequate information (including documentation necessary to complete the switching) and technical support; if problems are identified, the Provider and the Customer will in good faith analyse the causes and agree on solutions;
(b) act with due care to maintain business continuity and continue to provide the functions or Services under the Agreement (Article 25(2)(a)(ii) of the Data Act);
(c) maintain a high level of security throughout the switching process, in particular for the security of the Data during their transfer (Article 25(2)(a)(iv) Data Act).

1.6 Obligations of the Customer during the switching process

1.6.1 The Customer undertakes to take all reasonable measures to achieve effective switching. The Customer is responsible for importing Data and Digital Assets into their own systems or into the systems of the Destination Provider and implementing these Data and Digital Assets within these systems, including where the Customer uses the Services of a third party for these actions.

1.6.2 If applicable and without prejudice to Article 30(6) of the Data Act, the Customer and the Provider, or third parties mandated by them, undertake to respect the intellectual property rights of any materials provided in the switching process by the Provider, as well as the Provider's trade secrets. The Customer undertakes to provide access to and enable the use of these materials to third parties mandated by them only insofar as is necessary to complete the switching process and only upon the Provider's explicit authorisation. The access to and use of the Providers' materials related to the switching process which are protected by intellectual property rights and/or trade secrets related to the switching process will be terminated no later than at the end of the agreed transitional period, including the alternative transitional period, in full compliance with the confidentiality commitments and the intellectual property rights granted by the Provider.

1.6.3 The Customer acts in good faith to implement any guidance related to the switching process shared by the Provider.

1.6.4 The Customer may agree on successful switching metrics, as well as switching milestones with the Source Provider and informs the Source Provider about the extent to which these milestones have been achieved during the switching process. In any case, the Customer should inform the Provider that it has successfully completed switching.

In addition to the obligations in this Agreement, all Parties involved, including Destination Providers of Data Processing Services, have a legal obligation, laid down in Article 27 of the Data Act, to cooperate in good faith to make the switching process effective, enable the timely transfer of Data and maintain the continuity of Data Processing Services.

1.7 Unsuccessful switching

1.7.1 If the switching process is not successfully completed, Parties must cooperate in good faith to identify the cause and achieve successful completion, enable a timely transfer of Data and maintain continuity of the Services. In particular, upon the Customer's request, the Provider supports the Customer in identifying the reasons for unsuccessful switching and, to the extent the reasons identified relate to the Provider's environment or switching processes, advises how the technical problems identified can be solved. The rules applicable to switching charges apply to support provided by the Provider and other Provider's services referred to in this section.

1.7.2 The Customer may authorise the Destination Provider to act on their behalf.

1.8 Data retrieval and Data erasure

1.8.1 The Customer may retrieve or erase their Data during the agreed period for Data retrieval, which is […] days.

1.8.2 At the end of the agreed period for Data retrieval, and if the switching process has been successfully completed, the Provider erases all Exportable Data and Digital Assets generated by the Customer or directly related to the Customer. The Provider confirms [within x working days] that such erasure has been completed, except for the personal Exportable Data which the Provider is obliged to store under EU or national laws.

Data retrieval starts after the agreed transitional period is terminated and must be at least 30 calendar days after the termination of the transitional period that was agreed between the Customer and the Provider. The Customer may decide not to make use of their right to retrieve the Data. In such case, either it will erase the Data on its own (and may inform the Provider about it as stated in Article 25((3)(c) of the Data Act or the Provider will erase such non-retrieved Data as stated in clauses 1.8.2 of Option A and 2.7.2 of Option B).

1.9 Switching charges

1.9.1 The charges to be paid by the Customer for switching are as follows […]

In the event of in-parallel use of several Data Processing Services (multi-cloud deployment scenario), the Data Egress charges are not considered to be Switching Charges and as such can be imposed on the Customer for the purpose of passing on such costs incurred by the Provider, without exceeding the actual costs. In any other case, no switching charges can be imposed on the Customer after 12 January 2027 (see the explanations about switching charges included in the introductory information to this SCC).

1.10 Termination of the switching process

[See SCC Termination]

1.11 Notifications

The Parties agree any notification between them in respect of switching and exit to be done (*Parties fill in the chosen means of communication including by adequate electronic means*).

1.12 Order of precedence

In the event of any conflict or inconsistency between these clauses on switching and exit and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to switching between Data Processing Service, these clauses will take precedence.

2. Option B: Switching and exit with self-service automated switching tools

2.1 Information

2.1.1 Before placing the order for the Data Processing Services, the Provider has provided the Customer with clear information about:

(a) available self-service automated switching tools for such services ("Switching Tools") and the conditions of their use;

(b) their standard service fees and, where applicable, early termination penalties;

(c) the Switching Charges, including the fees for using the switching tools.

> Article 31 of the Data Act lays down a specific regime for certain Data Processing Services. For custom-built or highly individualised services, certain switching obligations do not apply. The Parties need to agree on how such switching could take place (including the cost). For Data Processing Services provided as a non-production version for testing and evaluation purposes and for a limited period of time the obligations for switching do not apply. While these standard contractual clauses were not drafted to cover such situations, they can still serve as inspiration for the Parties to an Agreement on such services.
>
> According to Article 30(6) of the Data Act, Providers will not be required to develop new technologies or services. Nor will they be required to disclose or transfer to a Customer or to a different Provider of Data Processing Services digital assets that: (i) are protected by intellectual property rights; or (ii) constitute a trade secret; or (iii) compromise the Customer's or Provider's security and integrity of service.

2.1.2 The switching checklist in **Appendix 2**, which forms an integral part of the Agreement, includes:

(a) an exhaustive specification of all categories of Data and Digital Assets that can be transferred with the use of Switching Tools, including at a minimum all Exportable Data (Article 25(2)(e) of the Data Act);

(b) an exhaustive specification of categories of Data specific to the internal functioning of the Provider's Data Processing Service that will be exempted from the Exportable Data where there is a risk of breach of the Provider's trade secrets (Article 25(2)(f) of the Data Act).

(c) information on procedures for switching and porting with the use of Switching Tools, including methods and formats, restrictions and technical limitations (including those arising from the storage of Data outside the EU), procedures, documentation, as well when applicable, best practices, capabilities, technical support which the Provider will make available to the Customer (especially during testing, preparation for switching and switching), including any hotlines available for Customers during switching or alternative communication channels and test scenarios; this information must explain how to switch all Exportable Data and Digital Assets in a coherent and consistent way quickly enough for effective switching;

(d) an estimate of the time needed to export and transfer the Data and Digital Assets out of the source Provider's environment, when the Switching Tools are used in accordance with the Provider's documentation;

(e) clear information concerning known risks to continuity in the provision of the functions or services on the part of the Source Provider (Article 25(2)(a)(iii) of the Data Act);

(f) the resources, including IT Resources (such as servers, CPU, memory, I/O, bandwidth), which will be provided by the Provider to ensure effective switching and the procedure for obtaining additional IT Resources.

2.1.3 The Provider provides the Customer with a reference to the on-line register with Data structures and formats, relevant standards and open interoperability specifications, where Exportable Data are available at [*specify link to the location]* (Article 26(b) Data Act).

2.2 Initiation of the switching process

2.2.1 The Customer initiates switching by sending the Provider a switching notice, as agreed in clause 2.10, observing the notice period [*Parties to indicate the agreed notice period, which cannot exceed two months*]. If the Customer wishes to switch only with regard to certain services and the corresponding Data or Digital Assets, this must be specified in the switching notice. [OPTION] [The Customer will give notice by using the form in **Appendix 3**.]

> The switching notice is a different instrument from a contract termination notice. Subject to the terms of the Agreement, the Customer may choose to switch only a certain subset of services provided by the Source Provider. In that case, the switching obligations concern only such services and the corresponding Data and Digital Assets; for the rest, the previously agreed contractual terms still apply.

2.2.2 In the switching notice, the Customer informs the Provider whether it intends:

(a) to switch to a different Provider of Data Processing Services; in this case the Customer should provide necessary details of the Destination Provider;

(b) to switch to an on-premises ICT infrastructure of the Customer; or

(c) not to switch but only erase their exportable Data and Digital Assets.

(d) [OPTION] [The Customer will give notice by using the form in **Appendix 4**]

2.2.3 The Customer may also indicate in the switching notice the time window(s) for switching and the additional IT Resources required by the Customer in such time windows. If the Provider is not able to ensure such IT resources in the indicated time-windows, it should object not later than [three working days] from receiving the switching notice, providing due justification and

propose several alternative "time-windows" to the Customer while respecting the maximum transitional period.

The time window(s) for switching is/are a period, for example a weekend, during which the Customer intends to make their systems unavailable for the users and no update occurs so that the Data are frozen, and the Customer may carry out the switching.

2.2.4 The Provider confirms to the Customer the receipt of the switching notice [within three working days] using the same means of communication as that used by the Customer.

The Customer may need to carry out the switching in a specific timeframe to minimise business disruption. Moreover, switching may require additional resources on the part of the Source Provider. Therefore, if needed, the Customer should indicate the time windows during which they intend to carry out switching and additional resources (in accordance with information provided by the Source Provider). If the Source Provider is not able to provide such resources within these time windows for justified reasons (e.g. scheduled maintenance of services which would severely affect the availability of resources during that time), they should provide the Customer with alternatives which would ensure effective switching by the end of the maximum transitional period.

2.3 Transitional period

2.3.1 When the Provider cannot respect the [mandatory maximum] transitional period because this is not technically feasible, the Provider undertakes to:

(a) notify in writing including by adequate electronic means, the Customer within 14 working days from [the date of the switching notice];

(b) indicate an alternative transitional period, which must not exceed seven (7) months from the date of the Customer's switching notice; and

(c) give proper justification for the technical unfeasibility.

The Customer confirms receipt of such extension notice [within three working days].

2.3.2 The Customer may extend the transitional period once, for a period they consider more appropriate for their own purpose, for no longer than [*specify the number of months*]. In that case, the Customer notifies the Provider in writing including by adequate electronic means, of their intention until the end of the original transitional period and indicate the alternative transitional period. The Provider confirms the receipt of such extension notice [within three working days].

[OPTION] [The Customer will give notice by using the form in **Appendix 5**;

2.4 Obligations of the Provider during the switching process

2.4.1 The Provider undertakes to provide reasonable assistance to the Customer and third parties authorised by the Customer in the switching process once the switching process starts and throughout it so that the Customer can switch within the transitional period. To this effect, the Provider must, in particular:

(a) act with due care to maintain business continuity and continue to provide the functions or Services under the Agreement;

(b) maintain a high level of security throughout the switching process, in particular, for the security of the Data during their transfer; and

(c) if problems are detected during the switching and cannot be resolved through technical support, together with the Customer, analyse the causes and agree on the solutions.

Even in option B "self-service automated switching tools" the Provider shares responsibility for the timing of the switching, for example, if the tools are too slow to ensure successful switching or if the Provider reacts with undue delay when the Customer detects a problem that requires the Provider's assistance.

2.5 Obligations of the Customer during the switching process

2.5.1 The Customer undertakes to take all reasonable measures to achieve effective switching. The Customer undertakes to be responsible for importing Data and Digital Assets into their own systems or into the systems of the Destination Provider and implementing these Data and Digital Assets including where the Customer uses the Services of a third party for these actions.

2.5.2 If applicable and without prejudice to Article 30(6) of the Data Act, the Customer and the Provider, or third parties mandated by them, undertake to respect the intellectual property rights of any materials provided in the switching process by the Provider, as well as the Provider's trade secrets. The Customer undertakes to provide access to and enable the use of these materials to third parties mandated by them only insofar as is necessary to complete the switching process and only upon the Provider's explicit authorisation. Access to and use of the Provider's materials related to the switching process which are protected by intellectual property rights and/or trade secrets related to the switching process will be terminated no later than at the end of the agreed transitional period, including the alternative transitional period, in full compliance with the confidentiality commitments and the intellectual property rights granted by the Provider.

2.5.3 The Customer may agree on successful switching metrics, as well as switching milestones with the Source Provider and informs the Source Provider about the extent to which these milestones

have been achieved during the switching process. In any case, the Customer should inform the Provider that it has successfully completed switching.

2.5.4 The Customer acts in good faith to implement any guidance related to the switching process shared by the Provider.

In addition to the obligations in this Agreement, all Parties involved, including Destination Providers of Data Processing Services, have a legal obligation, laid down in Article 27 of the Data Act, to cooperate in good faith to make the switching process effective, enable the timely transfer of Data and maintain the continuity of Data Processing Services.

The reasonable measures to achieve effective switching on the part of the Customer include, in particular:

- preparing the switching process internally (e.g. stopping all access to the Data and informing the user of the unavailability of the system; if a third party is entrusted with switching, providing appropriate instructions to such third party so that it respects the Agreement between the Customer and the Provider);
- monitoring the switching process (e.g. checking the exported Data and Digital Assets during switching to immediately identify any problems);
- appropriate contractual arrangements with the Destination Provider or ensuring appropriate resources for on-premises switching.

2.6 Unsuccessful switching

2.6.1 If the switching process is not successfully completed, Parties must cooperate in good faith to identify the cause and achieve successful completion, enable a timely transfer of Data and maintain continuity of the services. In particular, upon the Customer's request, the Provider supports the Customer in identifying the reasons for unsuccessful switching and, to the extent the identified reasons relate to the Provider's environment or switching processes, advises how the identified technical problems can be solved. The rules applicable to switching charges apply to support provided by the Provider and other Provider's services referred to in this section.

2.6.2 The Customer may authorise the Destination Provider to act on its behalf.

2.7 Data retrieval and Data erasure

2.7.1 The Parties agree that the Customer retrieves or erases their Data during the agreed period for Data retrieval, which is […] days.

2.7.2 At the end of the agreed period for Data retrieval, and if the switching process has been completed successfully, the Provider undertakes to erase all Exportable Data and Digital Assets generated by the Customer or related to the Customer directly and confirm to the Customer that it has done so, except for the Exportable Data which the Provider is obligated to store under mandatory EU or EU Member States laws as long as the Provider notifies the Customer, if allowed by the law, what Exportable Data they will retain, for how long and on what grounds.

Retrieval starts after the agreed transitional period is terminated and must be at least 30 calendar days after the termination of the transitional period that was agreed between the

Customer and the Provider. The Customer may decide not to make use of their right to retrieve the Data. In such case, either they will erase the Data on their own (and may inform the Provider about it as stated in Article 25(3)(c) of the Data Act or the Provider will erase such non-retrieved Data as stated in clauses 1.8 under Option A and 2.7 under Option B).

2.8 Switching charges

The charges to be paid by the Customer for switching are as follows […]

In the event of in-parallel use of several Data Processing Services (multi-cloud deployment scenario), the Data Egress charges are not considered to be switching charges and, as such, can be imposed on the Customer for the purpose of passing on such costs incurred by the Provider, without exceeding the actual costs. The testing tools for switching and the Provider's reasonable support of the Customer in testing as agreed in the Plan should be regarded as forming part of the switching process and consequently, the charges for such services should be gradually withdrawn in accordance with Article 29 of the Data Act.

2.9 Termination of the switching process

See Clause 1 in SCC Termination

2.10 Notifications

The Parties agree any notification between them in respect of switching and exit to be done [*Parties fill in the chosen means of communication including by adequate electronic means*].

2.11 Order of precedence

In the event of any conflict or inconsistency between these clauses on switching and exit and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to switching between Data Processing Services, these clauses will take precedence.

Appendix 1 – Switching and exit plan

1. **Contact details**

(a) Provider's contact for switching and exit: …

(b) Customer's contact for switching and exit: …

2. **The Customer must provide the following information in the written notice:**

(a) Data concerned by the notice, according to the agreed identification in **Appendix 2.**

(b) Destination of the Data: Customer's on-premises ICT infrastructure or a Destination Provider, including relevant technical specifications about the destination site.

(c) Location where the Data should be exported and transported.

3. **Provider's obligations to react to the written notice**

Within …. days, the Provider will reply to the Customer in writing, with the following information:

(a) Exhaustive specification of all categories of Data to be transferred during the switching process

(i) Exportable Data

- All Data imported by the Customer at the beginning of the Service Agreement including metadata (*input Data*)
  - A, with metadata: ….. in format ….
  - B, with metadata: ….. in format ….
  - C, with metadata: ….. in format ….
- All Data directly or indirectly co-generated by the Customer's use of the Data Processing Service:
  - D, with metadata: ….. in format ….
  - E, with metadata: ….. in format ….
  - F, with metadata: ….. in format ….

(ii) Digital Assets:

- L, in format …
- M, in format …

(b) Exhaustive specification of categories of Data specific to the internal functioning of the Provider's Data Processing Service that are to be exempted from the Exportable Data where a risk of breach of the Provider's trade secrets exists: ...

4. **Confirmation of the Data to be switched**

The Customer will indicate which Data and Digital Assets they want to receive within the agreed (or alternative) transitional period.

5. **Order, timing and testing**

During the transitional period:

(a) the agreed order and timing for exporting and transferring the chosen Data and Digital Assets is as follows: …
(b) description of the testing method proposed by the Provider: ....
(c) the Provider or the Customer using the Provider's tools and processes will test the export and transfer to the agreed location with part of the agreed Data and Digital Assets, to confirm or adapt the order and timing*;*
(d) the Customer will test importing into and implementation of the agreed Data and Digital Assets in their own systems or the systems of the Destination Provider;
(e) if there are problems with the testing or the results of the testing, the Source Provider and the Customer will determine whether they arise from the export of the agreed Data and Digital Assets and transfer processes under the Provider's responsibility or from their import and implementation processes under the Customer's responsibility.

6. **Execution of the switching process**

(a) The Provider must export and transport by electronic or physical means the Data or Digital Assets to the location specified by the Customer and the Customer (or any third parties the Customer has authorised) must import the Data or Digital Assets into their own systems or in the systems of the Destination Provider and implement these Data or Digital Assets within these systems.
(b) The Customer (or any third parties the Customer has authorised) must test the functionalities in their environment or the environment of the Destination Provider within .... *[Parties indicate the agreed period for conducting the test]* and document for the Provider any problems that arise from (i) the quality of the Data or Digital Assets exported or (ii) insufficient information given by the Provider.
(c) The Provider must react without undue delay so that the Customer can switch within the mandatory transitional period.

7. **Successful switching**

As soon as the Customer notifies the Provider that the switching process has been successfully completed, the Provider undertakes to notify the Customer without undue delay of the contract termination. If the Customer does not notify the Provider about successful switching or the lack thereof, while the Provider has grounds to believe that the switching was successfully completed by the Customer, the Provider may send the Customer a request for confirmation as to whether the successful switching has taken place. If the Customer does not confirm successful switching within 30 calendar days from such request, it is deemed that the switching was not successful, and the Agreement will not be terminated.

Appendix 2 – Switching checklist

Either the information required is explicitly mentioned hereunder or the information required can be found at […]

(a) Exhaustive specification of all categories of Data and Digital Assets that can be transferred including at a minimum all Exportable Data: ...

(b) Exhaustive specification of categories of Data and Digital Assets specific to the internal functioning of the Provider's Data Processing Service, with risk of a breach of the Provider's trade secrets, which are exempted from switching: ...

(c) Information on procedures for switching and porting with the use of switching tools: ...

(d) Estimate of the time needed to export and transfer the Data and Digital Assets: ...

(e) Known risks to continuity in the provision of the functions or services of the Source Provider: …

(f) IT Resources which will be ensured by the Provider for effective switching: ...

Appendix 3 – Switching notice

[Provider's name and address for communication]

[Date]

Switching notice

Name of Customer: […]

Contract: (*name and details of Contract, e.g. name of contract, its number, date of execution, as required by the Contract)*

Switched services: [*All covered by the Contract*] or [*provide explicit services or Digital Assets subject to switching if only part of the services are to be covered by switching*]

[OPTION] [On behalf of the Customer, I/we inform you that the Customer initiates switching of the switched services as of (*specify starting date*). The notice period is (*specified by the Customer: maximum two months, may be shorter at the Customer's discretion*.]

[OPTION] On behalf of the Customer, I/we inform you that the Customer initiates switching of the following services, Data or Digital Assets: …

[OPTION] The Customer informs you that it intends to switch to [*details of new provider/on premise infrastructure of Customer*].

[OPTION] [(*Applicable for automated switching*) The Customer would like to switch within the following time window(s): (*specify dates and details*). The Customer requests the following IT Resources to be available during such time windows (*to be completed by the Customer*).]

Contact details of person responsible for switching: (*details of Customer's representative responsible for switching process*).

_____

[signature of Customer's authorized representative]

Appendix 4 – Exit notice

This form is applicable if the Customer does not want to switch but only to erase their exportable Data or Digital Assets under both Option A and Option B.

[Provider's name and address for communication]

[Date]

Exit notice

Name of Customer: […]

Contract: [*name and details of Contract, e.g. name of Contract, its number, date of execution, as required by the Contract]*

Erased Data/ Digital Assets: [(*All covered by the Contract]* or [*provide explicit Data or Digital Assets subject to erasure]*

[OPTION] [On behalf of the Customer, I/we inform you that the Customer initiates switching consisting solely of erasure of Erased Data/Digital Assets as of (*starting date)*. The notice period is (*specified by the customer: maximum two months, may be shorter at the Customer's discretion)*].

[OPTION] [Contact details of person responsible for switching: (*details of Customer's representative responsible for switching process).*]

_____

[signature of Customer's authorized representative]

Appendix 5 – Notice for alternative transitional period

[Provider's name and address for communication]

[Date]

Notice for alternative transitional period

Name of Customer: […]

Contract: [*Name and details of contract. e.g. name of Contract, its number, date of execution, as required by the Contract]*

Erased Data/ Digital Assets: [*All covered by the Contract]* or [*provide explicit Data or Digital Assets subject to erasure]*

[OPTION] [On behalf of the Customer, I/we inform you that the Customer wishes to extend the transitional period to not later than (*date*].

[OPTION] [Contact details of person responsible for switching: (*details of Customer's representative responsible for switching process*).]

_____

[signature of Customer's authorised representative]

ANNEX VII: STANDARD CONTRACTUAL CLAUSES
on Termination

Regulation (EU) 2023/2854 (referred hereto as the Data Act) enables customers of Data Processing Services (i.e. cloud and edge computing services) to switch between providers or to transfer their Data to their own on-premises ICT infrastructure. The act of switching will have an effect on whether the Agreement between the Parties will continue or will be terminated.

These SCCs deal with the termination of the Agreement between the Customer and the Provider in relation to a particular service in the context of switching. These SCCs cover the Service contract termination process. They are directly linked to the SCCs Switching & Exit and provide for various termination possibilities and related conditions. The Data Processing Agreement is usually terminated (in full or partially) once the switching process has been successfully completed or if the Customer does not wish to switch to another Provider but requests all data to be erased and such erasure is successful. Some additional options are included in these SCCs to assist the parties under scenarios not covered in the Data Act.

The Agreement with the Provider may cover several services. If these SCCs are added to the Agreement and then the Customer switches one service to a Destination Provider while the other services remain with the Source Provider, the Agreement is terminated only in relation to this specific Service, unless the Parties agree otherwise.

In addition to the termination related to switching covered by these SCCs, the Agreement could also be terminated on any other grounds for termination included in the main Agreement or provided for by the applicable law. The Provider may decide to terminate the Agreement if the Customer breaches their obligations and tender a notice of termination. In this case, the Customer may provide a switching notice, with the result that the Agreement would be extended until successful completion of the switching process.

Other standard contractual clauses recommended by the Commission can be found attached hereto and they cover specific topics other than termination of the Agreement. The Parties are encouraged to consider using those other clauses, too, as they were developed to be consistent and reinforce each other.

What is included in the SCCs on Termination?

Scenarios provided by the Data Act: The Agreement will be terminated in specific circumstances once the switching has been concluded successfully (*Event A*) or if the Customer does not wish to switch but requires all Data to be erased and such erasure is successful (*Event B*). The Agreement will be considered terminated upon successful completion of switching (*Event A*) or at the end of the maximum notice period (*Event B*). There is no need to serve the termination notice or follow the termination procedure under the Agreement, as the Agreement will terminate automatically. The Provider is, however, obliged to notify the Customer that the Contract is considered terminated (Article 25(2)(c) of the Data Act). This notification is informative in nature, as the Agreement is already terminated. Thus, even if the Provider delays the notification, it cannot charge any fee under the terminated Contract.

However, the Customer should inform the Provider that the switching process was completed successfully, as the Provider may not be aware of this fact. If the Provider has reasons to suspect that the Customer has already successfully switched (e.g. the Customer is not logging into the service or, does not have any Data at rest stored in the service), the Provider may contact the Customer and request confirmation of successful switching. In the absence of a reply from the Customer, it is deemed that switching was not successfully completed and the Contract continues (i.e. it is not terminated) on its existing terms.

The Data Act does not define successful switching. In principle, it is up to the Customer to decide whether the switching was successful. However, the Customer, or the Customer and Provider, may agree to set certain criteria to assess whether switching was successful, in particular:

(a) completion of Data transfer i.e. whether all Exportable Data and, if applicable, Digital Assets have been transferred to the Destination Provider's environment, as well as whether their accuracy, integrity and completeness was maintained; the Exportable Data and Digital Assets should match the original Data and Digital Assets without any loss or corruption;
(b) deployment of Digital Assets (if applicable); if switching included transfer of Digital Assets, such as the Customer's own or licensed applications, the Customer should verify whether such Digital Assets are installed, configured and running in the Destination Provider's environment;
(c) testing of new service: in this phase, the Customer should verify whether the services offered by the Destination Provider work as planned before switching; in particular, the Customer should carry out the performance, functionality and operational testing of the Destination Provider's service, including switched Data or Digital Assets to assess whether its switching verification criteria are met.

In the case of a fixed-term contract, switching may end before expiry of the contract or after that (for the latter, see Event D). If switching ends before expiry of the contract, the Agreement will also expire. In that case, early termination penalties may be due (Articles (23a), 25.2(c) and 29(4) of the Data Act).

What if switching is unsuccessful?

See SCC Switching and Exit

To resolve a situation where switching is unsuccessful and the Agreement cannot be terminated, the Parties may submit a complaint to the competent authority under the Data Act, so that the authority takes a decision. However, it should be understood that the Parties can also use any legal means available within their jurisdiction (e.g. submitting a claim, requesting injunctions from civil courts, etc.).

Two further scenarios: Clauses 1.4 and 1.5 are optional, and present two further scenarios for the Parties to consider. While not expressly mentioned in the Data Act, these may occur in practice and are included in the clauses to help the Parties resolve such situations. These scenarios are as follows:

- The Customer wishes to extend the availability of their Data from the Source Provider or to maintain the Contract with the Source Provider using an option for buying a new service for a longer period, whether or not this is preceded by service switching or by a simple service termination without any switching. The Customer may need only a service of limited functionality from the Source Provider i.e. ensuring availability of their Data for this longer period or having a contract in place so that it is possible to order the new service (*Event C*).

In this case, as the Data will be available through a service of limited functionality, the Source Provider and the Customer should conclude a new Agreement for this additional service or amend the existing Agreement (see clause 1.4.2). In particular, the Parties should agree on a new period for Data Retrieval. In the case of general (framework) Agreements, the Customer may wish to keep the contractual relationship with the Source Provider in place in order to be able to quickly buy new services without going through the process of concluding a new Contract, which, in larger organisations, may be a lengthy and complicated process.

Example for Event C: The Customer has exported and transferred their Data successfully from the Source Provider to the Destination Provider in whose environment the Data were deployed successfully. Another example could be that the Customer may decide to terminate the service with the Source Provider without subsequently migrating to another Provider. In both examples the Customer, however, does not wish their Data

to be erased and rather prefers to have it backed up safely with the Source Provider extending beyond the agreed period for Data retrieval. Any such additional service enabled by the Source Provider does not prevent the termination of the original Agreement and the provision of the service would be based on a new or amended Agreement.

- A fixed-term contract expires before the switching process has occurred or has been completed (Event D)

Example for Event D: An example of this situation may be when the Customer does not provide notice sufficiently in advance. In this case, the Data has not been transferred to the Destination Provider on the date on which the Agreement with the Source Provider expires.

The Parties should be aware that a suspension of services may occur during the switching process. In this case, the general clause on suspension of services included in the Agreement applies.

Exemptions for certain custom-built services exist. See explanation accompanying the SCCs Switching and Exit.

1. Termination

1.1 Termination process

1.1.1 The Agreement will be considered terminated between the Parties when one of the following events has occurred:

(a) where applicable, on successful completion of the switching process. If successful completion of the switching process occurs before expiry of the agreed duration of the Agreement, the early termination fees set out in this Agreement will apply; or
(b) at the end of the maximum notice period where the Customer does not wish to switch but to erase its exportable Data and Digital Assets upon termination of the service.

1.1.2 If the Agreement contains any terms regarding termination subject to applicable law, such as mentioned below:

(a) a Party is applying for suspension of payments, or a Party has been declared bankrupt;

(b) a Party has not met, in a timely fashion, any obligation arising from the Agreement that results or could result (either by contract or by law) in termination of the Agreement;

(c) a Party has experienced a change of ownership or control that, by contract or by law, results or could result in termination of the Agreement;

(d) the Agreement is declared null and void as per a breach of or change in the applicable mandatory law; or

(e) any other situations that, by contract or law, result or could result in termination of the Agreement,

1.1.3 Even if during the switching process any ground for termination occurs, the Agreement and the agreed services and functions will not be terminated or expire before successful completion of the switching process (see clause 1.1.1(a)) or at the end of the maximum notice period, where the Customer wishes only to erase its Exportable Data and Digital Assets on the termination of

service (see clause 1.1.1(b) unless otherwise provided by mandatory law. This does not affect any other rights or remedies available to a Party towards the other Party. This also applies if the switching process starts after the Provider has tendered a notice of termination of the Agreement.

1.1.4 Without prejudice to other legal remedies available under applicable law, the Agreement will not be terminated or expire before successful completion of the switching process, or a relevant decision taken by a competent court or an agreement between Parties.

1.2 Termination upon completion of switching

1.2.1 The Agreement is not terminated until the switching process has been successfully completed. As soon as the Customer notifies the Provider that the switching process was successfully completed, the Provider without undue delay notifies the Customer of the termination of the Agreement.

1.2.2 If the Customer does not notify the Provider about successful switching or the lack thereof, while the Provider has justified grounds to believe that the switching was successfully completed by the Customer, the Provider may send the Customer the request for confirmation as to whether the switching was successfully completed. If the Customer does not confirm successful switching within 30 working days from such request, switching is deemed unsuccessful, and the Agreement is not terminated and continues on its existing terms.

1.3 Termination without switching

1.3.1 If the Customer does not wish to switch but to erase their Exportable Data and Digital Assets upon termination of the service, as set forth in clause 1.1.1(b), this can only occur and will be deemed completed, if:

(a) the [maximum] agreed notice period has expired and;

(b) the Customer has explicitly asked the Provider to execute the Data Erasure, and in response the Data has been successfully erased and this has been confirmed by the Provider;

(c) at the end of the agreed notice period the Provider has notified the Customer of the termination of the Agreement.

Other scenarios *[Optional clauses to be considered]*

1.4 Extended Data retention

1.4.1 At the end of the transitional period, the Customer may decide not to erase all their Exportable Data and Digital Assets at the end of the [minimum]/agreed period for Data retrieval and to

ensure that they will be available, including for the purpose of providing a service of limited functionality, for a specified extended period.

1.4.2 In this case, the Customer and Provider either agree (i) to amend the existing Agreement to cover the extended period for Data retrieval, or (ii) to conclude a new Agreement for service of limited functionality.

1.5 Expiry of a fixed-term contract before switching

1.5.1 If the Agreement was concluded for a fixed duration and i) the expiry date is reached before the switching process is completed, and ii) the Customer has not requested their Exportable Data and Digital Assets to be erased, then:

(a) the transitional period begins on the Agreement expiry date; the Provider provides reasonable assistance as set out in SCCs Switching and Exit;

(b) on successful completion of the switching process, clause 1.2 applies and;

(c) upon unsuccessful completion of the switching process, of SCC Switching and Exit clause 1.7 under Option A or clause 2.6 under Option B apply.

1.6 Notifications

The Parties agree that any notification between them in respect of these clauses on termination are to be done [*Parties fill in the chosen means of communication including by adequate electronic means]*.

1.7 Order of precedence

In the event of any conflict or inconsistency between these clauses on termination and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to termination of the Agreement underpinning the provision of Data Processing Services, these clauses will take precedence.

ANNEX VIII: STANDARD CONTRACTUAL CLAUSES
on Security and Business continuity

Recital 94 of Regulation (EU) 2023/285 (referred hereto as the Data Act) states that, throughout the switching process, a high level of security should be maintained, and that the Provider should act with due care to maintain business continuity and ensure the provision of the functions or Services under the Agreement, as well as to provide clear information concerning known risks to continuity.

The Data Act lays down obligations for the Provider to ensure a high level of security and business continuity with relation to the switching process. In particular, this concerns the security of Data during their transfer and the continued security of the Data during the retrieval period (Art. 25(2)(a)(iv) of the Data Act). While the topics of security and business continuity are generally included in the Data Processing Agreement and other contractual documentations, these SCCs focus on security and business continuity with relation to the switching and exit process as per the rights and obligations introduced by the Data Act.

These SCCs combine clauses on specific issues of security and business continuity throughout the switching process because of the similar context and spirit of both security and business continuity. Although provisions on security and business continuity are included in the Services Agreement, there are some specificities related to the switching process that must be reflected.

The switching process can give rise to particular security risks which may materialise during different phases of the switching process with respect to its different aspects to which special attention needs to be paid, such as:

i. Data processing;

ii. identity management and access control;

iii. Data transfer;

iv. Data retrieval;

v. ongoing Data confidentiality, integrity and availability; and

vi. other risks related to preparing for and executing an effective switching process.

Similarly, particular business continuity risks in relation to the switching process deserve special attention and consideration. These can concern:

i. maintaining business continuity to ensure a high level of Service security;

ii. continuing the provision of the Services under the Agreement;

iii. providing clear information concerning known risks to continuity in the provision of the Services.

In this respect, Article 25(2)(a)(ii) of the Data Act obliges the Provider to act with due care to maintain business continuity and ensure the provision of the functions or Services under the contract. The Provider is also obliged to provide clear information concerning known risks to continuity in the provision of the functions or Services on the part of the source provider of Data Processing Services (Article 25(2)(a)(iii) of the Data Act).

Risk-based security and business continuity: Where the SCCs provide for contractual arrangements, a risk-based and all-hazards approach regarding security implies a dynamic and contextual approach to applicable Services and deployment models and related use, needs and risks. It is up to the Customer and the Provider to jointly identify, agree upon, implement and monitor the related measures and controls in order to ensure improved overall Service resilience and integrity.

For instance, special attention will need to be given to continuous appropriate and accountable levels of:

i. Data integrity;

ii. resilience to all known vulnerabilities when making Data available for retrieval;

iii. encryption signatures;

iv. special multi-factor access management;

v. verification of identity, including authorisation;

vi. security of website, portal, platform and related Application Programming Interfaces (APIs) ;

vii. Provider-side security;

viii. provision and assurance of the Customer side, including the relevant Destination Provider(s)' security;

ix. network activity;

x. brute force registration;

xi. Transport Layer Security (TLS), and other in-transit security;

xii. Distributed denial-of-Service (DDOS) protection; and

xiii. strong Data erasure policies and practices.

The Provider should be able to demonstrate, for the Customer's benefit, that the technical, operational and organisational measures on security and Data protection are provided in a continuous and appropriate manner.

This idea is similar to the structure and approach in (i) Article 25 GDPR and Article 32 GDPR [Regulation - 2016/679] respectively; (ii) the NIS2 Directive [EUR-Lex)], (iii) cybersecurity certification scheme under the Cybersecurity Act (EU) 2019/881.

Examples of what the Provider should demonstrate include:

i. internal security, assurance monitoring and security breach or other incident handling policies

ii. compliance with certain open, non-proprietary standards as commonly used in the relevant sector;

iii. certification or other assurance in accordance, or other compliance, with the either relevant applicable national law or relevant European cybersecurity certification schemes developed under Regulation (EU) 2019/881 (the Cybersecurity Act); or

iv. regulatory technical standards, if and where applicable in the relevant sector(s).

Risk-based regulations: For many Providers operating in the EU, as well as for some Customers, certain risk-based regulations may apply. This generally results in increased levels of security obligations and responsibilities, with breaches and other incidents resulting in more severe legal, reputational and other consequences. Therefore, consideration of these risk-based regulations is highly recommended before entering into a Services Agreement and during its execution.

Some examples of risk-based regulations that may apply are : the NIS2 Directive (NIS2), Critical Entities Resilience Directive (CER), the Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), Cybersecurity Act and General Data Protection Regulation (GDPR) as well as possible rules under national laws.

These SCCs use the term "Incident" in relation to both security and business continuity (*see section "Definitions"*).

Clause 1.4 encompasses, for example, also notifications under Article 33 of the GDPR, Article 23 of NIS2.

Other standard contractual clauses recommended by the Commission can be found attached hereto and they cover other specific topics than security and business continuity. The parties are encouraged to consider using those other clauses, too, as they were developed to be coherent and reinforce each other.

1. Security and Business Continuity

1.1 General

1.1.1 The Provider undertakes to apply the most appropriate technical and organisational measures to ensure that the level of security and resilience is proportionate to the risks presented by the Services and their intended and reasonably foreseeable use with respect to the switching process.

1.1.2 Furthermore, the Provider undertakes to prevent Service disruptions and maintain continuity of the Services during the switching process. This includes having and maintaining adequate business continuity management that includes contingency planning and disaster recovery measures based on established best practice and market standards. These measures must be kept up to date and periodically reviewed and tested by the Provider.

1.2 Security

1.2.1 Further to clause 1.1.1, the Provider must implement appropriate technical and organisational measures to ensure that a high level of security is maintained during the switching process. This relates, in particular, to the security of Data during their transfer and continued security of the Data during the period for Data retrieval.

1.2.2 The Provider must implement appropriate technical and organisational measures to maintain during the switching process a level of security proportionate to the level of risks. This includes:

(a) relevant risks related to the security of Data Processing, identity management and access control, Data portability, Data retrieval, ongoing Data confidentiality, integrity and availability as well as any other risks related to effective switching.

1.2.3 Measures covered in clauses 1.1.1 and 1.2.1 must at least ensure, without limitation:

(a) ongoing confidentiality, integrity, availability of the Data and resilience of the Services, Exportable and Digital Assets;

(b) restoration of the availability and integrity of the Data and access to them in a reasonably timely manner in the event of an Incident; and

(c) continuous monitoring as well as regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of the Services, Exportable Data and Digital Assets.

1.3 Business continuity

1.3.1 Further to clause 1.1.2, the Provider must in particular:

(a) act with due care to maintain business continuity and continue to provide the Services under the Agreement; and

(b) provide clear information concerning known risks to continuity in the provision of the Services.

1.4 Notifications

1.4.1 The Parties agree any notification between them in respect of these clauses on security and business continuity to be done [*Parties fill in the chosen means of communication including by adequate electronic means]*.

1.4.2 The Provider must notify the Customer of any Incidents. The Provider must notify without undue delay and in any event within 72 (seventy-two) hours of becoming aware of the Incident, unless regulatory obligations require a warning or similar notification within a shorter period.

1.4.3 The Provider's notification must include the information required for the Customer to assess the consequences of the Incident. The Provider must promptly, effectively, reasonably and at no additional cost, assist and cooperate with the Customer (including with third parties authorised by the Customer) regarding any investigation action the Customer is entitled to undertake in accordance with applicable EU and national law.

1.4.4 Where the Provider is affected or is likely to be affected by an Incident, the Provider must take the most appropriate action necessary to minimise the impact of the Incident and prevent it from recurring. This does not affect other rights that the Customer may have under the Agreement or under applicable EU or national law.

1.5 Miscellaneous

1.5.1 At the Customer's request, the Provider must, without undue delay, provide the Customer with a summary of the key elements of the Provider's security measures and related security management, as well as of its business continuity and related contingency management and of any material changes to any of the above.

1.5.2 At the Customer's request, the Provider must without undue delay provide the Customer with additional details complementing the above-mentioned summary, such as test results and assurance evidence. In this case, the Provider may require the Customer to sign a non-disclosure Agreement before sharing such details. This non-disclosure Agreement must however include customary exceptions and be without any effect on the other terms of this paragraph, the Agreement or applicable EU or national law. The Provider has the right to request that the details be shared on a need-to-know basis only, including with its Designated Provider(s) or other relevant third-party suppliers of the Customer.

Such customary exceptions include any (relevant part of) information (i) that is already in the public domain, (ii) the Customer is obliged to disclose where it is mandatory to do so (a) by applicable law, or (b) by any governmental or other regulatory authority (the latter two including without limitation court order, GDPR, NIS2).

1.6 Order of precedence

Without prejudice to the standard contractual clauses under the GDPR, in the event of any conflict or inconsistency between these clauses on security and business continuity and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to security and business continuity, these clauses will take precedence.

ANNEX IX: STANDARD CONTRACTUAL CLAUSES
on Non-Dispersion

Data Processing Agreements often comprise of various ancillary documents referring to additional material and information that can be widely dispersed across different repositories. This makes it difficult for prospective Customers to find all the information they need in order to assess the 'Parties' contractual and legal obligations and their implications.

In the context of the switching process, transparency is very important. A prospective Customer needs easy access to relevant updated information, documents, materials and contact details, even before concluding a contract with the Provider. The SCCs Non-Dispersion provide for information and communication symmetry.

These SCCs help the easy and practical access to relevant updated information, documents, materials and contact details by both Customer and Provider. They aim to create an environment of transparency between the Parties, and to ensure that there are no contractual obstacles to switching, by allowing the Customer to find all relevant and updated information about their rights and obligations in the Agreement. This will contribute to a fair and balanced legal relationship between the Customer and the Provider and, in general, to contractual fairness, as advocated for in Regulation (EU) 2023/285 (referred hereto as the Data Act).

Other standard contractual clauses recommended by the Commission can be found attached hereto and they cover specific topics other than dispersion. The parties are encouraged to consider using those other clauses, too, as they were developed to be consistent and reinforce each other.

1. Non-Dispersion

1.1 Introductory conditions & arrangements

1.1.1 The Provider ensures that all contractual arrangements are easily, readily and continuously available and accessible for the Customer (a) in one dedicated secure online location, and (b) in a comprehensible, human readable as well as machine-readable format. In addition, the Provider ensures that the contractual arrangements are downloadable or otherwise exportable for the Customer in a complete and structured manner.

1.1.2 Contractual arrangements must include, at least:

(a) **Name & address:** the Provider's full official corporate name as a legal entity, including, without limitation, its official legal form, national registration number, full official address and a VAT registration number;

(b) **Up-to-date Agreement:** the current, time-stamped (and where available execution copies of the) Agreement, including all terms, accepted offers, conditions, policies, information, documentation, schedules, exhibits and annexes that are applicable between the Provider and the Customer;

(c) **Historical record:** the historical record of the time-stamped Agreements, coupled, if possible, with any ancillary terms, conditions, including any policies, information, documentation, schedules, exhibits, annexes or other that have been applicable between the Provider and the Customer

(i) including evidence of Permitted Unilateral Changes and the respective Permitted Unilateral Change effective dates as set forth by SCCs Non-amendment.

> For Permitted Unilateral Changes and the respective Permitted Unilateral Change effective dates see SCCs Non-Amendment

(d) **Data Processing & supply ecosystem:** the up-to-date historical record and detailed list of subcontractors, data processors and/or other relevant supply chain ecosystem stakeholders of the Provider, including names and addresses as in clause 1.1.2 (a) above;

(e) **Contact details:** the current contact details of the Provider including details of functions of the primary key contact, primary technical contact and primary contract and administrative contact, including the respective function titles, phone numbers and email addresses agreed by the Parties;

(f) **Operational performance reporting:** where technically feasible, an up-to-date as well as historical overview of the operational performance reporting by the Provider on the Service provided and other obligations under the Agreement; and

(g) **Notification:** any legal and other relevant time-stamped notifications between the Parties or to a Party related to the contractual arrangements as in clause 1.1.2 (a) and (b)

> In several situations, the Data Act obliges the Provider to provide required information to the Customer. These obligations are reflected in the relevant SCCs. For example, information regarding the available procedures for switching and transferring Data (Article 26 of the Data Act) is included in the SCCs Switching and Exit; the obligation to provide clear information concerning known risks to the continued provision of functions/services is reflected in the SCCs Security and business continuity and in the SCCs Switching and Exit.

1.2 Order of precedence

In the event of any conflict or inconsistency between these clauses on non-dispersion of applicable contractual documentation and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to the topic of these clauses, these clauses will take precedence.

ANNEX X: STANDARD CONTRACTUAL CLAUSES
on Liability

While a clause on liability is usually included in the general Agreement between the Customer and the Provider, the provisions of these SCCs on liability reflect the spirit of Regulation (EU) 2023/2854 (referred hereto as the Data Act) as regards the importance of fair, reasonable and non-discriminatory rights and obligations, and as such may be a useful complement to the standard provisions of an Agreement on liability.

Therefore, the inclusion of such a clause is recommended as it is essential for the balance of the contractual relationship between the Parties and provides incentives for compliance with the rights and obligations agreed by the Parties. In particular, small and mid-size companies and other organisations may find these SCCs helpful when they agree on liability provisions in their Agreements. The Customer and the Provider are free to agree on additional rights and obligations in their Contract. The use of this clause does not dispense the Parties from ensuring compliance with any applicable mandatory provisions of EU or national law and adapting them accordingly.

Before concluding an Agreement, the Customer may check the insurance market for the most appropriate insurance product for their needs. Seeking advice from an expert specialised in insurance is recommended.

Other standard contractual clauses recommended by the Commission can be found attached hereto and they cover specific topics other than liability. The Parties are encouraged to consider using those other clauses, too, as they were developed to be coherent and reinforce each other.

Unlimited liability

As a rule, each Party to the Agreement should bear unlimited liability in cases of intent, wilful misconduct or gross negligence, including a Party's breach of obligations of confidentiality of the other Party's Data or obligations not to use Data for purposes other than those explicitly agreed by the Parties.

The SCCs recommend separating the cases where the breach is intentional, and where it is caused by wilful misconduct and making it clear that all intentional actions are covered, irrespective of the law governing the Contract. In some jurisdictions, wilful misconduct may be synonymous with intent. In such cases, the Parties may decide not to differentiate between wilful misconduct and intent.

Waivers to unlimited liability

Data Processing Services provided as non-production versions for testing and evaluation purposes and for a limited time (Article 31(2) of the Data Act), are usually not intended for the processing of sensitive data (for instance, trade secrets, personal data or actual production Data). Such non-production versions are also generally not sufficiently developed for such processing and lack capabilities, controls and configuration that could reasonably be expected in the production version. The Customer is strongly discouraged from processing actual production Data in such non-production versions. These SCCs propose that, if the Customer decides to do so, this is at their own risk and that the Provider is not liable if a breach of Data confidentiality occurs in such cases. In this situation, specific liability arrangements agreed by the Parties may apply.

Similarly, the Data Act envisages situations when certain obligations do not apply to services where most of the main features have been custom-built, where all components have been developed for an individual Customer, or for s provided in a non-production environment. As a consequence, the liability for those cases would also need to be expressly agreed upon.

Limited liability

It is current business practice that the Parties agree to limit their liability (especially, the Provider's) in some cases. These SCCs propose three main options to limit liability:

- **Option A:** Liability is limited to the amount identified by the Parties based on a risk assessment. Under this option, both Parties perform a risk assessment and provide its findings to the other Party in the pre-contractual phase. The other Party may reject the risk assessment received. If the risk assessment is rejected, the Parties may apply one of the other options for limiting liability.
  There may be changes in the volume of services received from the Provider, as well as a change of scope (adding new services or removing some services). This may require changes to the risk assessment and the Parties should adapt the liability limit to reflect the actual risk situation. The Parties are encouraged to check the example of the risk assessment template under Option A so that they are aware of the risks related to Data Processing Services for their particular business.

- **Option B**: Liability is limited to direct damages. Consequential damages such as loss of profit or missed savings are excluded. This option can also be combined with Options A and C (i.e. limit liability to direct damages but not higher than an amount set by the parties either following a risk assessment or determined on another basis).

- **Option C**: The Parties' liability is limited to a pre-agreed maximum amount, which can be calculated, for example, on the basis of (i) the equivalent of single / multiple annual fees (paid and due) by the Customer to the Provider;; (ii) the insurance coverage as taken out by the Provider related to the services;; (iii) the maximum amount as covered by the Provider's general professional liability insurance;; or (iv) a combination of different formulas, e.g. a formula linked to the services' monetary value multiplied by the amount equal to the annual overall fees (either paid or (not yet) due under the Agreement) for the services.

Indemnification: These SCCs do not include provisions on indemnification. The Parties are encouraged to consider whether and, if so, to what extent a Party may need to indemnify and hold the other Party harmless from any claims of third parties caused by or relating to a material breach of obligations under the Agreement by acts or omissions of the liable Party, its employees, representatives or subcontractors. In the case of Customers, the indemnification may apply, for instance to the Provider's breach of its confidentiality obligations non-use or infringement of third-party intellectual property rights. For Providers, the indemnification may cover the Customer's breach of third party intellectual property rights or third party claims to the Provider related to the hosting of illegal content by the Customer.

12. Liability

1.1 Unlimited liability

1.1.1 In cases of breach of the obligations under this Agreement committed with intent or caused by wilful misconduct or gross negligence, the Party in breach is liable for all damages, subject to clause 1.2 below. [OPTION] [Except as stipulated in clause 1.2, the Provider is liable without

limitation for all damages caused to the Customer by a breach of the confidentiality of the Customer's Data processed under this Agreement.]

1.1.2 In the case of a breach of the obligation not to use a Party's Data for purposes other than those expressly agreed by the Parties, the Party in breach is liable for all damages without limitation.

The intention behind the option included under clause 1.1.1 is to guarantee the confidentiality of all Customer Data in accordance with the confidentiality rights and obligations and to the extent agreed in the Agreement. As per applicable law (for instance, GDPR, NIS2 etc.), a recipient of confidential information may have certain obligations to disclose certain information to certain persons / organisations for purposes agreed and explicitly described in the Agreement.

1.2 Waivers of unlimited liability

1.2.1 If the Parties agree unlimited liability as per clause 1.1.1, the Provider's unlimited liability does not apply to Customer Data in a non-production version of the Provider's Data Processing Services.

See Article 31(2) of the Data Act and explanatory note 'Waivers to unlimited liability' of this SCC.

1.2.2 The Provider is not liable for:

(a) obligations not applicable to Data Processing Services under (i) Article 23(d) of the Data Act (achieving functional equivalence); (ii) Article 29 (gradual withdrawal of switching charges); or (iii) Articles 30(1) and (3) of the Data Act (technical aspects of switching) if most of the main features in the Provider's Data Processing Services are custom-built to accommodate the Customer's specific needs or where all components have been developed for the Customer's purposes, and where those Data Processing Services are not offered at broad commercial scale via the service catalogue of the Data Processing Services. The waiver applies if the Provider has informed the Customer before the conclusion of the Agreement for Data Processing Services that the above provisions of the Data Act do not apply to said services;

(b) a breach of the obligations related to switching between Data Processing Services to Data Processing Services provided as a non-production version for testing and evaluation purposes, and for a limited period of time.

1.3 Limited liability

Option A: Amount determined by a risk assessment

1.3.1 The Parties agree to limit their liability in the case of negligent breach of obligations under this Agreement to the amount of […] per event, including when a series of connected events applies as one event. The amount is determined by the aggrieved Party in good faith on the basis of a risk assessment or other estimations agreed by the Parties in Annex 1 (Risk assessment template). The risk assessment is conducted and provided to the other Party [.... days] before

concluding the Agreement. If the risk assessment is not rejected by the other party, the Agreement is concluded on this basis.

The Parties may agree at any time to re-assess the risks to reflect changes in the risk situation with regard to the services. For this, they may use the template set out in the example [Risk assessment template]. If the re-assessment results in an increase or decrease of the risk for the Party, that Party may ask to negotiate the liability cap for the services to reflect the change in the risk associated with them or additional conditions that should be met, which may include pricing or amendments to the agreed Service-level Agreement. The Parties could agree that, if no Agreement is reached within [three months from the Party's request], the initially agreed liability cap will remain unchanged.

Option B: Direct damages

1.3.2 The Parties agree to limit their liability in the case of a negligent breach of obligations under this Agreement to any direct damages caused.

1.3.3 Direct damages also include: (i) costs incurred in order to determine the cause and extent of the damages; (ii) costs incurred by the aggrieved Party in order to prevent or limit direct damages, provided that those costs actually led to their being prevented or limited; (iii) damage on account of corrupted, unavailable or lost Data; and (iv) costs incurred by one Party in order to ensure that the services meet the levels of use as agreed in the Agreement, if the other Party has not remedied such breach within the agreed time.

1.3.4 Where a series of connected events applies as one event, the one Party's aggregated liability towards the other Party for such direct damages as laid down in the previous sentence is limited to the amount of […].

Option C: Maximum amount

1.3.5 The Parties agree to limit their liability in the case of a negligent breach of obligations under this Agreement, including when a series of connected events applies as one event, to a maximum amount of […].

1.4 Notifications

The Parties agree that any notification between them in respect of these clauses on liability is to be done (*Parties fill in the chosen means of communication including by adequate electronic means*).

1.5 Order of precedence

In the event of any conflict or inconsistency between these clauses on liability and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to liability within the scope of these clauses, these clauses will take precedence.

Appendix 1 – Risk assessment template

To determine the risks associated with the service, a Party conducts an assessment taking into account the specific risks of negligent non-performance by the other Party under the Agreement.

This risk assessment has to be made in good faith. It should realistically reflect potential damages. Where the estimated amounts are too low, liability for higher damages will be excluded. Where the estimated amounts are too high, the other Party may refuse to accept liability or require higher costs.

Additional risks may be included where necessary.

Risk description		**Damage estimate**
Business interruption Loss of turnover caused by a breach of contract. A potential service downtime and its implications on the Party's business or operations may be considered.	EUR	
Data recovery Assumed costs for recovery of lost, unavailable or corrupted Data. Parties may be required to implement measures to mitigate their risks, e.g. by having backup Data at another Provider or on the premises.	EUR	
Government fines Government fines against business are, for instance, fines for violation of data protection laws or regulatory provisions resulting from the Provider's operation of the service.	EUR	
Loss of business secrets The disclosure of business secrets can result in loss of business opportunities. Such damages may be recoverable by law.	EUR	
Breach of personal data and remediation actions A personal data breach can lead to several types of direct costs related to legal fees, litigation costs as well as data remediation efforts to eliminate any data quality issues related to the breach.	EUR	

Loss of reputation Parties may consider the impact on the company's reputation and what measures will be necessary (e.g. advertising and campaigning to compensate for the reputational impact). Such costs may be difficult to recover fully in court proceedings.	EUR	
Third-party liability Third-party liability covers potential liability, for instance towards suppliers, customers, subcontractors and third parties.	EUR	
Total risk of potential damages (sum)	**EUR**	

As Data Processing Services are provided in a scalable and elastic manner, both the use of the service provided by the Provider and the liability risk may vary over the course of the Agreement, often within the range in the service-level agreements. When assessing the risks at the time when the Agreement is concluded or on a recurring basis, the Parties are advised to reflect the changing nature and volume of the services in addition to the potential maximum theoretical damages. This would allow for a more realistic value for average or expected use of service. Parties should also align the assessment with their internal planning. Not all risks categories listed may equally apply to a Customer and Provider or to a Customer's specific line of business.

ANNEX XI: STANDARD CONTRACTUAL CLAUSES
on non-amendment

It is important that the Parties can rely on the contractually agreed rights and obligations and that these rights and obligations are not changed unilaterally, unless under clearly and mutually agreed conditions. This is especially true for small and medium-sized enterprises or other organisations, which may not have sufficient resources to assess the possible impact of these unilateral changes on their activities and mission. The SCCs Non-Amendment are intended to give more clarity and confidence to the Parties when agreeing on terms pertaining to unilateral amendments. These standard contractual clauses address relevant scenarios and possible contractual arrangements associated with them. They are intended to ensure that such unilateral amendments are not detrimental to the interests of either Party.

Approach to unilateral amendments

As a general rule, the Agreement (including the SCCs) cannot be unilaterally amended by either Party and they need to be mutually agreed. Only under strict conditions as provided for in these SCCs, are certain unilateral amendments allowed. This is reflected in clauses 1.1.1 to 1.1.3 of these SCCs.

These SCCs acknowledge that in certain circumstances the Provider should be able to propose unilateral amendments to the services provided. These are called Permitted Unilateral Amendment(s) and are set out in clauses 1.1.3 to 1.1.6 of these SCCs. A Permitted Unilateral Amendment (s) can only be proposed once and should meet the following conditions:

1. It/they improve(s) the Customer's position in respect of their use of the service from the contractual, financial, organisational, operational, service-level, legal compliance or other point of view; and
2. It is/they are notified to the Customer no later than 30 calendar days before any such proposed Permitted Unilateral Amendment(s) will be effective for the Customer.

The notification period will allow the Customer to assess the information, as well as the feasibility and impact for the Customer and the Customer's stakeholders, systems and services.

Other standard contractual clauses recommended by the Commission can be found attached hereto and they cover specific topics other than non-amendment. The parties are encouraged to consider using those other clauses, too, as they were developed to be coherent and reinforce each other.

1. Non-amendment

1.1 Amendment

1.1.1 Any amendment to the Agreement ('Amendment') must be made in writing, including by adequate electronic means, and will be subject to prior mutual consent, including by adequate electronic means.

1.1.2 Notwithstanding clause 1.1.1, the Provider is entitled to amend the Agreement if this is required to comply with mandatory applicable law not already in force before the effective date of the Agreement's entry into force.

1.1.3 Except as provided for in clause 1.1.2 the Provider is only entitled to propose a Unilateral Amendment to the s, provided that:

(a) such Amendment is beneficial for the Customer's use of the data processing services, for instance by consisting of material enhancement updates of the Service or being necessary for security reasons; and

(b) all the conditions set out in clauses 1.1.4 to 1.1.6 (‘Permitted Unilateral Amendment’) have been met.

1.1.4 No proposed Unilateral Amendment under clause 1.1.3 may be used by the Provider to directly or indirectly implement or enforce retroactive changes, or to amend clauses in the Agreement pertaining to one or more of the following aspects regarding:

(a) choice of law and choice of forum;

(b) amendments or procedure for amending the Agreement;

(c) term and termination;

(d) liability;

(e) confidentiality;

(f) methods for the use of subcontracting and methods for the change of subcontractors;

(g) access and information rights;

(h) qualitative service level objectives;

Changes regarding already agreed quantitative and qualitative service performance targets within the agreed service levels with associated penalties and/or service credits may be proposed as a Permitted Unilateral Amendment as per clause 1.1.3.

(i) pricing rules or other financial rules;

A change toto the agreed fees may be proposed as a Permitted Unilateral Amendment as per clause 1.1.3 but the underlying rules, such as the price indexation methodology, itself have to be mutually agreed by the parties,

(j) the location where the Data are processed or stored if that location is outside the EU.

Changes between EU locations can be agreed by the Parties from the beginning of their contractual relationship or can be proposed by the Provider as a Permitted Unilateral Amendment. However, when the location where data are processed or stored changes from a location within the EU to a location outside the EU or from a location outside the EU to another location outside the EU, the Parties should mutually agree this change.

1.1.5 In the event of a proposed Permitted Unilateral Amendment, the Provider must:

(a) notify the Customer no later than 30 calendar days unless otherwise required by the applicable law before the proposed Permitted Unilateral Amendment takes effect;

(b) provide the Customer in a clear and comprehensible manner, with information including:

(i) the scope, details and timelines of the proposed Permitted Unilateral Amendment;

(ii) why the proposed Permitted Unilateral Amendment is required, including with respect to its benefit for the Customer’s use of the data processing services;

(iii) the difference between the prevailing situation and the situation after the proposed Permitted Unilateral Amendment. This includes, in particular, any contractual,

financial, organisational, operational, service-level and legal compliance-related consequences for the Customer, if any;

> The description of such a difference should address the expected situation with respect to the relevant types of existing customers, taking into account the categories indicated under clause 1.1.5(b)(iii). This is to ensure that the most likely implications of a notified Unilateral Amendment are visible to and understood by the Customer. In this respect, this clause does not require the Provider to notify an assessment tailored to individual Customers.

(iv) the envisaged timeline for deployment and implementation, and the related effective date of the proposed Permitted Unilateral Amendment entering into force.

1.1.6 If the Provider fulfils the conditions of clause 1.1.5 the Customer will be deemed to have accepted the proposed Permitted Unilateral Amendment at the Permitted Unilateral Amendment effective date.

1.1.7 If the Provider breaches clauses 1.1.2 to 1.1.5 in respect of amending the Agreement, the Customer will have the right to terminate the Agreement at no additional cost and to obtain compensation for the damage suffered (including the costs for switching to another provider of data processing services). This does not affect the Customer's other rights and remedies, including with respect to seeking injunctive relief in any applicable competent court to order the Provider to continue providing the services as agreed and to obtain damages suffered, if any.

> If the amendment of the Agreement by the Provider is not in line with the contractual provisions, the Customer should have the right to terminate, which, in practice, should also imply tendering a switching notice to initiate the switching process (see SCCs Switching and Exit Option A if the Parties had agreed on a Switching and Exit Plan and Option B in the case of self-service automated switching). However, in such cases, the Customer should be entitled to recover the damages it suffered by being 'forced' to switch to another provider, including the costs it incurred and other related damages (see SCC Liability).

1.2 Notifications

The Parties agree any notification between them in respect of these clauses on non-amendment to be done (*Parties fill in the chosen means of communication including by adequate electronic means*).

1.3 Order of precedence

In the event of any conflict or inconsistency between these clauses on non-amendment and any other applicable contractual arrangements, terms, conditions or other applicable Agreements related to changes to the Agreement within the scope of these clauses, these clauses will take precedence.

ANNEX XII: STANDARD CONTRACTUAL CLAUSES
Definitions

For the purpose of the SCCs, the terms used will be defined as follows:

'Agreement' means the written Agreement between Parties in respect of the provision of services, any amendment thereof or supplement thereto, as well as all acts related to the performance of the Agreement(s), including, in particular its Appendixes;

'Appendix' means an appendix, schedule or exhibit explicitly referenced in the Agreement;

'Customer of Data Processing Services (Customer)' as defined in Article 2(30) Data Act means a natural or legal person that has entered into a contractual relationship with a Provider of Data Processing Services with the objective of using one or more Data Processing Services;

'Data' as defined in Article 2(1) Data Act means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording;

'Data Act' means Regulation (EU) 2023/2854;

'Data egress charges' as defined in Article 2(35) Data Act mean Data transfer fees charged to Customers for extracting their Data through the network from the ICT infrastructure of a Provider of Data Processing services to the system of a different provider or to on-premises ICT infrastructure;

'Data Processing Service' as defined in Article 2(8) Data Act: means a digital service that is provided to a Customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction. For purposes of this Agreement, the said Data Processing Services regard those provided or to be provided by the Provider to the Customer as agreed under the Agreement;

'Destination Provider', as mentioned in Article 2(34) Data Act, means the destination provider of Data Processing Services to which the Customer of a Data Processing Services changes for the purpose of using another Data Processing Service of the same Service type, or other Services;

'Source Provider', as mentioned in Article 2(34) Data Act, means the legal entity with whom the Customer has entered into a contractual relationship regarding the provision of Data Processing Services and other Services by the Provider under the Agreement, and from which the customer now intends to change to another provider;

'Digital assets', as defined in Article 2(32) Data Act, mean elements in digital form, including applications, for which the Customer has the right of use, independently from the contractual relationship with the Data Processing Service it intends to switch from;

'Exportable Data', as defined in Article 2(38) Data Act, means the input and output Data, including metadata, directly or indirectly generated, or cogenerated, by the Customer's use of the Data Processing

Service, excluding any assets or Data protected by intellectual property rights, or constituting a trade secret, of Providers of Data Processing Services or third parties;

‘Incident’ means a physical, technical, or organisational security breach, incident or similar event that may have a significant impact in relation to security and business continuity as it has caused or is capable of causing severe disruption of any applicable IT systems and operations used between the Provider and the Customer during the switching process, or with respect to the Customer’s use of the Services, the Customer’s Exportable Data and Digital Assets. See SCCs Security and business continuity

‘Interoperability’, as defined in Article 2(40) of the Data Act, means the ability of two or more data spaces or communication networks, systems, connected products, applications, Data Processing Services or components to exchange and use data in order to perform their functions;

‘Metadata’, as defined in Article 2(2) of the Data Act, means a structured description of the contents or the use of data facilitating the discovery or use of that data;

‘Non-personal data’, as defined in Article 2(4) of the Data Act, means: Data other than Personal data;

‘On-premises ICT infrastructure’, as defined in Article 2(33) Data Act, means ICT infrastructure and computing resources owned, rented or leased by the customer, located in the data centre of the customer itself and operated by the customer or by a third-party;

‘Other Services’ means all professional Services of whatever nature provided by the Provider to the Customer under the Agreement as defined therein, that are not Data Processing Services;

‘Party’ means either the Customer or the Provider;

‘Parties’ means both the Customer and the Provider;

‘Personal Data’ as defined in Article 4(1), of Regulation (EU) 2016/679 (General Data Protection Regulation (‘GDPR’));

‘Plan’ means the switching and exit plan referred to in the SCC Switching and Exit Option A, as agreed between the Parties under the Agreement;

‘Processing’, as defined in Article 2, point 7 of the Data Act, means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or other means of making them available, alignment or combination, restriction, erasure or destruction;

‘Provider of Data Processing Services (Provider)’ means a natural or legal person that has entered into a contractual relationship with a Customer with the objective of providing one or more Data Processing Services;

‘Same Service Type’, as defined in Article 2(9 of the Data Act, means a set of Data Processing Services that share the same primary objective, Data Processing Service model and main functionalities;

‘Services’ means both the Data Processing Services as well as all Other Services as agreed by Parties under the Agreement;

‘Service Fee’ means the fees due and owed by the Customer to the Provider as consideration for the provision of Services as agreed by the Parties under the Agreement;

‘Switching’, as defined in Article 2(34,, of the Data Act, means the process involving a source Provider of Data Processing Services, a Customer of a Data Processing Service and, where relevant, a Destination Provider of Data Processing Services, whereby the customer of a Data Processing Service changes from using one Data Processing Service to using another Data Processing Service of the same Service type, or other Service, offered by a different provider of Data Processing Services, or to an on-premises ICT infrastructure, including through extracting, transforming and uploading the Data;

‘Switching charges’, as defined in Article 2(36,, of the Data Act mean charges, other than standard Service fees or early termination penalties, imposed by a provider of Data Processing Services on a customer for the actions mandated by the Data Act for switching to the system of a different provider or to on-premises ICT infrastructure, including Data egress charges.