
# Final Report of the Expert Group on B2B data sharing and cloud computing contracts

2 April 2025

This document has been prepared for the European Commission, however it reflects the views only of the members of the Expert Group who contributed as independent experts and not representing their employer and/or organisations. The European Commission is not liable for any consequence stemming from the reuse of this publication.

© European Union, 2025

The Commission's reuse policy is implemented under Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39, ELI: http://data.europa.eu/eli/dec/2011/833/oj).
Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

# Introduction

## I. Context

### The Expert Group

According to Article 41 of the Data Act the Commission should recommend non-binding model contractual terms on data access and use ('MCTs') and standard contractual clauses for cloud computing contracts ('SCCs'). In 2022 the Commission set up the Expert group on B2B data sharing and cloud computing contracts to assist it with the development of the terms and clauses.

The expert group consists of 17 members acting in individual capacity, mostly lawyers, but also other practitioners and academics with experience in contracts for sharing data between companies and in cloud computing services. The experts started by identifying together the issues to be covered by the models, collecting use-cases, industry standards and similar or related contractual models and exchanging based on their own experience.

The first meeting of the Expert Group was held in September 2022. Until the end of March 2025 the Expert Group met 19 times in an official format, chaired by the Commission services that ensured the secretariat of the group. In between these meetings, the experts worked in smaller drafting group for each clause, which was afterwards discussed during the plenary meetings.

### The sub-group

The Commission also set up a sub-group comprising of companies, European and nation-wide organisations active in data sharing and cloud computing. The sub-group gave feedback to the experts throughout the drafting process. All draft terms and clauses that the Expert Group prepared were subject to consultation with the sub-group, sometimes several times, and their input was then considered by the experts in view of improving the texts.

### Consultation activities

In addition to the feedback received via the sub-group, the draft terms and clauses were also subject to consultation via a testing exercise organised during summer 2024. 12 companies provided feedback on the MCTs and 14 on the SCCs. The experts debated the results and made changes to the drafts where needed.

In November and December 2024 the Commission organised a series of six public webinars, where several members of the Expert Group presented the MCTs and SCCs. Between 200 and 300 participants took part in each webinar and participants had the opportunity to express opinions, drafting suggestions and elaborate with examples. Following these webinars, the experts further improved the drafts.

## II. Nature and use of the clauses

The MCTs and SCCs are non-binding, voluntary and have been drafted so they can be adapted by the parties according to their contractual needs. However, the parties need to consider that these models were drafted to be in line with the rights and obligations provided by the Data Act and were also designed to be coherent with each other. The various models include information about their voluntary nature and warnings to the parties to consider the legal consequences when making changes. They are accompanied by an introduction with explanations and instructions about how best to use them.

The model terms and clauses were drafted mainly for business-to-business relations. However, they can be used also in relations between business and consumers but, in that case, 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 case of contracts concluded online/at a distance).

### III. MCTs

The experts analysed chapters II-IV of the Data Act and drafted the following MCTs to help implement these provisions:

- Data Holder to User
- User to Data Recipient
- Data Holder to Data Recipient
- Data Sharer to Data Recipient

### IV. SCCs

Article 41 of the Data Act refers to the need for non-binding standard contractual clauses for cloud computing contracts to assist parties in drafting and negotiating contracts with fair, reasonable and non-discriminatory contractual rights and obligations.

Following this approach, the experts have considered the provisions of chapters VI and VIII and identified several contractual issues that are relevant for both the practical effectiveness of the newly introduced customer's right to switch and exit as well as for the fairness and contractual balance between parties. As opposed to the approach for the MCTs, where the Expert Group drafted full contracts, the Expert Group drafted six standard clauses to cover the main contractual issues identified for the cloud computing contracts and one general clause. These clauses are meant to be inserted by the parties into the data processing services agreements.

1. General
2. Switching & Exit
3. Termination
4. Security & Business continuity
5. Non-dispersion
6. Liability
7. Non-Amendment

### V. How to use the MCTs and SCCs

When considering using these models, the parties should first read the explanations and examples included to facilitate understanding and to reflect on the most common business situations. Some models contain several options for a given term/clause.

The parties should reflect on their specific needs, business relation and interests to identify the right option that best suits their contract. Usually, such options are accompanied by guidance and examples to explain the differences between them and when they are most likely to be appropriate.

# MODEL CONTRACTUAL TERMS

## I. Purpose of the model contractual terms

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

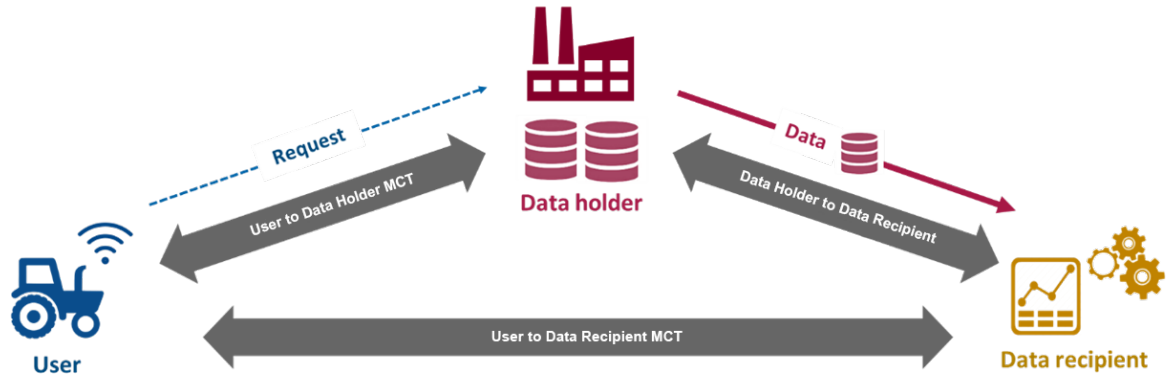
These MCTs were developed by a group of experts set up by the European Commission.

These models are non-binding and voluntary in nature. The parties to a contract can complement and adapt the MCTs set out in the Annexes to their individual needs and to specific EU and Member State law, where such specific law applies.

Passages marked in grey and italics indicate that details need to be filled in by the parties.

Passages marked with [OPTION] or *(if applicable)* may be appropriate or not, depending on the individual situation and preferences; note that also many terms not marked in this way may be derogated from by the parties.

## II. Which MCTs to use for which type of data sharing




The model contractual terms in Annex I 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 model contractual terms in Annex II 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 model contractual terms in Annex III 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 modifications where a data holder is obliged to make data available to a third party data recipient under other EU law or national legislation adopted in accordance with EU law.


The model contractual terms in Annex IV 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 parties should identify their own situation by reference to the different scenarios explained above and then use the relevant MCTs.

### III. Legal value of the MCTs in relation to Data Act and other applicable law

The MCTs seek to ensure compliance with EU and Member State law, in particular with the Data Act[1], the Data Governance Act[2] and the Trade Secrets Directive[3]. Use of the model contractual terms by contracting parties does not affect any of the rights and obligations they have under the Data Act or under other EU law or Member State law adopted in accordance with EU law, including obligations of the controller and the rights of data subjects under the General Data Protection Regulation (GDPR).[4]

The parties should pay particular attention when sharing of data concerns personal data or mixed datasets. Parties are advised to refer to the "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union" (COM/2019/250 final), which addresses these notions. Especially in relation to mixed datasets, it clarifies that "if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the GDPR fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset". In particular, data holders shall make available personal data to users or third parties, as mandated under the Data Act, but only as long as there is a legal basis in accordance with the GDPR.

As for any contract, use of the model contractual terms by 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 EU or Member State law.

1 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access and use and amending Regulation (EU) 2027/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023).

2 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)

3 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)

4 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 119/1, 4.5.2016, p. 1–88).

## IV. Who are the Parties to the model contractual terms

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

For the voluntary data sharing MCT, the experts chose to use the term 'data sharer' to take into account the multiple scenarios that are possible here.

For more information on the various roles and their definition, please consult the Commission's FAQ document on the Data Act.

## V. List of annexes and appendixes

Annex I: Model Contractual Terms for contracts on data access and use between data holders and users of connected products and related services

- Appendix 1 contains details of the data covered by this contract and of access arrangements
- Appendix 2 contains the form for an access request by the User
- Appendix 3 contains the form for a request to make data available to a third party
- Appendix 4 contains details of measures for the protection of trade secrets
- Appendix 5 contains details on sharing data with third parties
- Appendix 6 contains details of protection measures
- Appendix 7 contains details on compensation of the User
- Appendix 8 contains details on penalties
- Appendix 9 contains documentation on ownership of the Product or contractual rights to use the Product or Related services

Annex II: Model Contractual Terms for contracts between Users and Data Recipients

- Appendix 1 contains a description of the Data
- Appendix 2 lists the protective measures to be taken by the Data Recipient
- Appendix 3 contains information on sharing the Data with third parties by the Data Recipient
- Appendix 4 contains information on compensation to the User for the Data Recipient's use and sharing of the Data
- Appendix 5 contains documentation on ownership of the Product or contractual rights to use the Product or Related services

Annex III: 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

- Appendix 1 contains evidence on the request and, if applicable, any mandate
- Appendix 2 contains details of the Data covered by the contract and access arrangements
- Appendix 3 contains details of the calculation of compensation, including the potential status of the Data Recipient as an SME
- Appendix 4 contains details of measures for the protection of trade secrets
- Appendix 5 contains details on penalties

Annex IV: Model Contractual Terms for contracts for voluntary sharing of data between business Data Sharers and Data Recipients

- Appendix 1 contains a description of the Data
- Appendix 2 contains further details regarding Data covered by a regime requiring specific measures
- Appendix 3 contains details on Personal Data and respective obligations of the Parties
- Appendix 4 contains applicable security measures for the sharing of Data

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

The Data Act aims to promote sharing of data (personal and non-personal) generated by or in relation to products connected to the internet, which "*may be used and reused for a variety of purposes and to an unlimited degree*" (Recital (1)). This set of terms is meant to address data access and use and related contractual matters that may arise between a data holder and users (as defined by the Data Act).

The Data Act grants users of such products and related services new rights, i.e. to access data directly or via the data holder and to share data with third parties.

Articles 4(13) and 4(14) of the Data Act also specify that a data holder may only '*use any readily available data that is non-personal data*' and/or '*make available non-personal product data to third parties*' for commercial or non-commercial purposes provided this was contractually agreed upon with the user.
The terms below that cover these situations are likely to be needed for all connected products and related services.

Other 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, so they 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 when relevant, i.e. if otherwise the security requirements of the product would be undermined, resulting in a serious adverse effect on the health, safety or security of natural persons.

## 1. Parties and Product/Related Service

### 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 holder' 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 acts therefore as the 'Data Holder'; in the absence of an agreement with the User, the other parties are considered as

third parties within the meaning of clause 7.2. 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 7.2.1.

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 below collectively as 'the Parties' and individually as 'the Party'.

According to the Data Act, '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. This set of terms 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 may be inclined to look very closely at whether the procedure is designed in a way that is fair and that makes the terms and conditions become part of the contract.

### 1.2 Product/Related Service

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)*.

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 shall not require that a natural or legal person 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 (the 'Data') consist of any readily available Product Data or Related Service(s) Data within the meaning of the Data Act.

The Data consist of the Data listed 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, new data are 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.
>
> '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 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 any 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 benefit);

(b) providing support, warranty, guarantee or similar services or to assess User's, Data Holder's or third party's 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, including artificial intelligence (AI) solutions, 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 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 complement it.

The User should assess the consequences of such uses for their operations and their legitimate interests and also whether they should be remunerated by the Data Holder, especially when the Data Holder may freely use and sell the Data generated by the User.

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 then – not be covered by this provision;
- **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. The use of the Data for independent product development by third parties on the Data Holder's side would require either that those third parties enter into a separate contracts with the User if they are Data Holder or that the provision allowing sharing Data with such third parties for their own purposes be added below.

The Parties should agree – ideally in a separate section – on the interdependencies between Data use and functionalities of the Product or Related Service. In drafting the relevant passages, the Data Holder/the Parties should be aware that the courts may be particularly critical of excessive tying or bundling and may strike down contractual clauses they consider to be abusive or unfair.

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 e.g. 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 sharing of the data with particular (categories of) third parties; and/or
- The use of the data for particular purposes.

None of the Data uses agreed to under clause 3.1.1 may be interpreted as including such Data use, and the Data Holder undertakes to ensure, by appropriate organisational and technical means, that no third party, within or outside 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 The Data Holder may share with third parties the Data [OPTION] [as specified in **Appendix 5**] and which is non-personal data, if:

(a) the Data is 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 admissible purposes the third parties can pursue for their own needs, independently from the Data Holder, and whether the data is 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 previous clause 3.2.1 (a);

ii) to comply with clause 3.1.2;

iii) to apply the protective 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, or unless such Data sharing is required, in the interest of the User, to fulfil this Contract or any contract between the third party and the User] [OPTION 2] [not to share these Data further except as set forth in **Appendix 5**. Further details, including with regard to 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**.] If the User agrees to the further transfer, the Data Holder should oblige the third party with whom they share Data to include the clauses corresponding to points (i) to (iv) in their contracts with recipients.

3.2.2 The Data Holder may always 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 the agreed purposes under clause 3.1. The third parties may also use such services to achieve the agreed purposes under clause 3.2.1 (a).

### 3.3 Use and Sharing of Personal Data by the Data Holder

The Data Holder may use, share with third parties or otherwise process any Data that is personal data, under 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).

### 3.4 Protection measures taken by the Data Holder

3.4.1 The Data Holder undertakes to apply the protective measures for the Data [OPTION 1] [that are reasonable in the circumstances, considering the state of science and technology, potential harm suffered by the User as a result of Data loss or disclosure of Data to unauthorised third parties and the costs associated with the protective measures.] [OPTION 2] [that are set out in detail in **Appendix 6**, which forms an integral part of this Contract.]

> Parties should consider whether they wish to include, if needed in a separate Appendix, all the details of how important interests 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.

3.4.2 The Data Holder may also apply other appropriate technical protection measures to prevent unauthorised access to Data and to ensure compliance with this contract.

3.4.3 The User agrees not to alter or remove such technical protection measures unless agreed by the Data Holder in advance and in writing.

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

These clauses 3 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, the following clauses 7 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 made using the form specified in **Appendix 2**, sent to (*describe modalities for a simple request through electronic means where technically feasible*).

The form specified in Appendix 2 is one possibility for users to make a request but the parties can agree on alternative procedures. It illustrates the details a request may contain.

4.1.2 The Data Holder shall make the Data which is personal data available to the User, when the User is not the data subject, only when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (GDPR) 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 (EU)2002/58) 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 at least the same quality as it becomes 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.

The Data Holder must specify the Data characteristics and inform the User of these specifications in **Appendix 1**.

> 'Metadata' means a structured description of the content or the use of data facilitating the finding or use of those data.
>
> Though the relevant metadata needed to interpret and use those data are not laid down and must therefore be decided on by the Parties 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)).

4.2.2 The Data Holder and User may use the services of a third party (including a third-party providing Data Intermediation Services as defined by Article 2 of Regulation (EU) 2022/868) 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, unless they process the Data for its own business purposes. The party requiring the use of such a third party must notify the other party in advance.

4.2.3 The User must receive access to the Data:

(a) easily and securely [OPTION 1] [by the Data being transmitted] [OPTION 2] [by access to the Data where it is stored];

*(if applicable)* (b) without undue delay after the Data becomes available to the Data Holder; and

*(if applicable)* (c) [OPTION 1] [continuously and in real-time] [OPTION 2] [with appropriate frequency].

The Data Holder must specify these access arrangements and inform the User of these specifications in **Appendix 1**.

4.2.4 The Data Holder must provide to the User, at no additional cost, the means and information strictly 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 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.

In order to meet these requirements, the Parties agree on the specifications set out in **Appendix 1**, which forms an integral part of this Contract.

> The Data Holder must provide for free the means and information strictly necessary for the exercise of the right to access Data in accordance with article 4.

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.

### 4.3 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 4.2.3 or of **Appendix 1** on the Data quality and access arrangements and if the User notifies 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 of the incident. If the incident was caused by a failure of the Data Holder to comply with their obligations, they must remedy the breach [OPTION 1] [within a reasonable period of time] [OPTION 2] [within a time period of (*specify*)]. If the Data Holder does not do so, it is considered as a fundamental breach and the User may invoke clause 12 of this contract (remedies for non-performance). 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.

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 within a reasonable timeframe, it allows the user to use the contractual remedies provided for by the Contract in case of fundamental breach of the contract.

The clause also draws attention to User's right to lodge a complaint with the competent authority in accordance with Article 37(5), point (b) of the Data Act. However, the user should be aware that the 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 which is the most appropriate way to oblige the Data Holder to comply with its legal and contractual obligations.

### 4.4 Unilateral changes by the Data Holder

The Data Holder may, in good faith, unilaterally change the specifications of the Data or the access arrangements stated in **Appendix 1**, if this is objectively justified by the general 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.

The Data Holder must in this case give notice of the change to the User [OPTION 1] [without undue delay] [OPTION 2] [within *(indicate a reasonable period of time)*] after deciding on the change. Where the change may negatively affect Data access and use by the User more than just to a small extent, the Data Holder must give notice to the User at least *(indicate a reasonable period of time longer than the period in the first sentence)* before the change takes effect.

A shorter notice period may only suffice 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.

### 4.5 Information on the User's access

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; and

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

## 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 is considered to be protected as a trade secret, as this would subvert the intended effects of the Data Act.

   *See clauses 5.1.1, 5.1.2, 5.1.3, 5.1.4 and 5.4.1.*

2. **Trade secrets** – However, if the Data Holder identifies that certain Data covered by this contract is protected as trade secrets, they are entitled to certain rights, primarily to continue to preserve the confidentiality of the secrets in question by implementing reasonable steps as provided for by the Trade Secrets Directive (EU) 2016/943.

   To see which Data is protected as a trade secret and how to define a 'trade secret holder', see Article 2(1) of the Trade Secrets Directive.

   *See clause 5.1.1.*

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 is identified in the Contract. The Data Holder must therefore inform the User prior to concluding this contract with the User.

   *If yes, see clause 5.1.2 and the other clauses hereunder cater for that.*

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.

   *For such cases, clause 5.1.4 and the other clauses hereunder cater for that.*

5. **Audit rights -** In order to preserve the confidentiality of the Data protected as trade secrets, while not interfering with each other's activities, certain audit rights by means of involving independent third parties may be considered, including mechanisms in case of

disagreements related to the results of the audit report. The parties may use alternative measures to audits.

*See clause 5.2.3.*

6. **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, 5.3 and Appendix 4.*

7. **Trade secret holder rights (2/4)** – If the initial measures do not suffice, the trade secrets 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 5.4.2.*

8. **Trade secret holder rights (3/4)** – The trade secrets 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 5.4.3.*

9. **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 5.4.4.*

10. **Retention of Data containing Identified Trade Secrets** – If the Data Holder withholds or suspends data sharing in accordance with clauses 5.4.2, 5.4.3 or 5.4.4, the Data Holder will still be obliged to keep the related Data containing Identified Trade Secret readily available by retaining it up to the moment that it can be shared within scope of the Contract.

    *See clause 5.6.*

11. **Third party identified trade secret holder** – if the trade secrets holder is a third party, the Data Holder must make sure that Clause 6 also protect their trade secrets and obtain all relevant authorisations by said third party trade secrets holder.

    *See clause 5.1.3.*

### 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 clauses 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 (EU) 2016/943), held by the Data Holder or another Trade Secret Holder (as defined in said Directive).

5.1.2 The Data protected as trade secrets (hereafter referred to as 'Identified Trade Secrets') and the identity of the Trade Secret Holder(s) are set out in **Appendix 4**, which forms an integral part of this Contract.

5.1.3 The Data Holder hereby declares to the User that they have all relevant authorisations and other rights from the third party Identified Trade Secrets Holder to enter into this Contract regarding the applicable Identified Trade Secrets and all of the related rights and obligations under this Contract.

> According to Article 2(1) of the Trade Secret Directive, the term 'Trade Secret' means information which meets all of the following 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 protected as Trade Secrets if the Data Holder or the Trade Secret Holder took such steps before any request made in accordance with article 4 of the Data Act.

5.1.4 If, during this Contract, new data are made available to the User that is 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 the Trade Secret Appendix has been amended and agreed between the Parties, the Data Holder may temporarily suspend the sharing of the specific newly Identified Trade Secret(s) by giving notice to the User and the competent authority designated under Article 37 of the Data Act, with a copy of this sent to the User.

5.1.5 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

> Parties should, in a separate appendix as part of the Contract, include all the details of these measures. Measures may be both technical (e.g. encryption, firewalls, split storage, etc.) and organisational (e.g. internal governance, appropriate identity management and access controls, 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 access is to be provided where the Data are stored or the Data are to be fully transferred to the user. In the former case, the Data Holder or a trusted third party has a higher degree of control and can apply part of the protective measures themself, 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.

5.2.1 The User must apply the protective measures set out **Appendix 4** (hereinafter: 'Identified Trade Secrets U Measures').

5.2.2 If the User is permitted to make Data protected as Trade secrets available to a third party, the User must inform the Data Holder of the fact that Identified Trade Secrets have been or will be made available to a third party, specify the Data in question, and give the Data Holder the identity and contact details of the third party.

5.2.3 [OPTION] [In order to verify if and to what extent the User has implemented and is maintaining the Identified Trade Secrets U Measures, the User agrees to either (i) annually obtain, at User's expense, a security conformity assessment audit report from an independent third party chosen by the User, or (ii) to annually allow, at 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 User's compliance with availability, integrity, confidentiality principles as further described in the Trade Secrets Appendix 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 the User opts for a security audit from an independent third party at Data Holder's expense as set forth above, it retains the right to obtain security audit report from an independent third party at User's expense if it deems the security audit report from an independent third party at Data Holder's expense is not correct. If this right is exercised, both independent third-party auditors, together with Parties, will discuss any difference between those two reports and aim to resolve any pending materials matters while observing good faith.]

This clause is optional, because the parties may agree other measures in order to verify User's compliance with their obligations to implement and maintain Identified Trade Secrets U Measures.

### 5.3 Protective measures taken by the Data Holder

5.3.1 The Data Holder may apply any appropriate technical and organisational protection measures set out in detail **Appendix 4** to preserve the confidentiality of the shared and otherwise disclosed Identified Trade Secrets (hereinafter: 'Identified Trade Secrets DH Measures').

5.3.2 The Data Holder may also add unilaterally appropriate technical and organisational protection measures, if they do not negatively affect the access and use of the Data by the User under this contract.

5.3.3 The User undertakes not to alter or remove such Identified Trade Secrets DH Measures, unless otherwise agreed by the Parties.

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

5.4.1 The Data Holder must share the Data, including Identified Trade Secrets, in accordance with this Contract, and may not refuse, withhold or terminate the sharing of any Identified Trade Secrets, except as explicitly set forth in the clauses 5.4.2, 5.4.3 and 5.4.4.

5.4.2 Where the Identified Trade Secrets U Measures and the Identified Trade Secrets DH Measures do not materially suffice to adequately protect a particular Identified Trade Secret, the Data Holder may, by giving notice to the user with a detailed description of the inadequacy of the measures:

(a) unilaterally increase the protection measures regarding the specific Identified Trade Secret in question, provided this increase is compatible with its obligations under this Contract and does not negatively affect the User, or

(b) 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 of such measures is duly substantiated, e.g. in a security audit report, the Data Holder may suspend the sharing of the specific Identified Trade Secret by giving notice to the User and to the competent authority designated pursuant to Article 37 of the Data Act, with copy of this sent to the User.

The Data Holder must continue to share any Identified Trade Secrets other than these specific Identified Trade Secrets.

5.4.3 If, in exceptional circumstances, the Data Holder is highly likely to suffer serious economic damage from disclosure of a particular Identified Trade Secret to the User despite the Identified Trade Secrets U Measures and the Identified Trade Secrets DH Measures having been implemented, the Data Holder may stop sharing the specific Identified Trade Secret in question.

They may do this only if they give a duly substantiated notice to the User and to the competent authority designated pursuant to Article 37 of the Data Act, with a copy being sent to the User.

However, the Data Holder must continue to share any Identified Trade Secrets other than those specific Identified Trade Secrets.

> 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 e.g. the lack of enforceability of trade secrets protection in non-EU countries, the nature and level of confidentiality of the Identified Trade Secret in question or the uniqueness and novelty of the relevant connected product.

5.4.4 If the User fails to implement and maintain their Identified Trade Secrets U Measures and if this failure is duly substantiated by the Data Holder, e.g. in a security audit report from an independent third party, the Data Holder is entitled to withhold or suspend the sharing of the specific Identified Trade Secrets, until the User has resolved the incident or other issue as described in the following two paragraphs.

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

On receiving this notice, the User must address the incident/issue without undue delay (i.e., they must (i) assign the appropriate priority level to the incident/issue based on its potential detrimental impact and (ii) resolve the issue in consultation with the Data Holder and otherwise in accordance with the applicable proceedings as set out in **Appendix 4**).

5.4.5 Clause 5.4.2 does not entitle the Data Holder to terminate this contract.

Clauses 5.4.3 or 5.4.4 entitle the Data Holder to terminate his contract only with regard to the specific Identified Trade Secrets, and if:

(i) all the conditions of clause 5.4.3 or clause 5.4.4 have been met;

(ii) no resolution has been found by Parties after *(insert 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

(iii) the User has not been awarded by a competent court with 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 request the User:

(a) to 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 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 under clauses 5.4.2, 5.4.3 and 5.4.4 the Data Holder exercises the right to withhold, suspend or in any other way end or refuse the data sharing to the User, it will need to ensure that the particular Data that is the subject matter of the exercising of such right is retained, so that said Data will be made available to the User:

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

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

Above 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 in part or in full where and to the extent the withholding, suspension or refusal to provide data was caused by the User acting in bad faith**.**

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

### 6.1 Permissible use and sharing of data

The User may use the Data made available by the Data Holder upon their request for any lawful purpose and/or share the Data freely subject to the limitations below.

### 6.2 Unauthorised use and sharing of data

6.1.1 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 with that intent;

(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 to obtain access to Data or, for that purpose, abuse gaps in the Data Holder's technical infrastructure which is designed to protect the Data;

(d) share the Data with a third-party considered as a gatekeeper under article 3 of Regulation (EU) 2022/1925;

(e) use the Data they receive for any purposes that infringe EU law or applicable national law.

6.1.2 [OPTION] [Furthermore and in accordance with article 4 (2) of the Data Act, the User and the Data Holder agree to restrict the following processing, which could undermine security requirements for the Product, as laid down by EU or national law, resulting in a serious adverse effect on the health, safety or security of natural persons (*specify concerned processing*) having as a consequence to undermine (*specify concerned legal security requirement*) resulting in (*specify concerned serious adverse effect on the health, safety or security of natural persons*), the User undertakes not to (specify concerned restriction related to the above-mentioned processing). The Data Holder declares to the User that the competent authority designated under Article 37 of the Data Act has been duly notified of any of these restrictions, that result in a refusal to share the Data.]

## 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 its behalf. The request can be made using the form specified in **Appendix 3**, sent to (*describe modalities for a simple request through electronic means where technically feasible*).

7.1.2 The Data Holder shall make the Data which is personal data available to a third party following a request of the User, when the User is not the data subject, only when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (GDPR) 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 (EU)2002/58) 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 at least the same quality as they become 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 under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with Chapter III and Chapter IV of the Data Act.

7.1.5 The User acknowledges that a request under clause 7.1 cannot benefit a third party considered as 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].

## 8 [OPTION at the discretion of the User] 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)*.

> The Data Act 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"* (Recital (25)).
>
> This statement should be read in accordance with article 7(2) clarifying that "*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.*"

Therefore, the User may at its sole discretion accept or refuse the limitation(s) under this clause. Such additional limitations on the use and sharing of the Data agreed upon by the User will only be valid if they do not cause any detriment to the User and if the User receives a proportionate compensation in return (see clause 9).

As a consequence, this clause may apply in exceptional cases, if the User has an interest in agreeing to specific and limited restrictions, for instance if the Data Holder and the User engage in a joint industrial project.

In addition, this clause should not deprive the User from their legal rights under articles 4 and 5 of the Data Act. The User could not, for instance, waive their right to access data in accordance with article 4 of the Data Act. The User could only agree on specific limitations on the use of the Data accessed to in accordance with this article. As indicated in recital 25, the User could for instance accept to not further share the data with a third party.

## 9 Compensation to the User

### 9.1 Compensation

The Data Holder undertakes to compensate the User as set out in detail in **appendix 7**, which forms an integral part of this Contract, *(if applicable)* including for the limitations of User's rights in accordance with clause 6.3.

The parties can agree on a 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 a 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. Reversely, if for instance the Data is used exclusively for the needs of any agreement concluded with the User or for ensuring the functioning, the safety and the security of the Product or Related Service, a compensation might not be included.

However, the parties should be aware that, for example, if the User limits their rights in accordance with clause 6.3, the User must be compensated, as explained in the explanatory box under clause 6.3, and the compensation must be proportionate to the value of the limitation,

Similarly, parties should be aware that 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 7.2.1 (a) (iii).

If a compensation is due, the parties must agree on its form.

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

In case of delay with payment of compensation, 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 foreseen by the applicable law.

## 10 Transfer of use and multiple users

The Initial User may transfer permanently 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 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 car to customers.

In such cases, the Data Holder must conclude a contract with the Subsequent or Additional Users to be entitled to use non-personal data generated by the use of the Product or Related Services by such Users.

**Straightforward situation: each user needs an account**

Using the Product or Related Services may require the user to possess an account with the Data Holder (for example with an identity, login and password created via the product or on an app/software). Each user will be required to enter a contract with the Data Holder on creating the account. In such cases, no action from the initial user is required in case of a transfer, apart from a notification that they lost their quality as a user and that the contract with the Data Holder terminates and making sure that other users (defined below) will not be able to use the initial user's account. This may involve removing credentials before handing over the product or granting rights to the Related Services.

**Complex situation: an account is not needed by each user**

Users may be able to use the Product or Related Services without having an account with the Data Holder, meaning the Data Holder is unable to identify who is using the Product or Related Service.

This is a difficult situation as the subsequent user would not know of and could not agree to the use or making available of the Data by the Data Holder, in the absence of a contract with the Data Holder (for example, in the case of a connected vehicle which can be used without authentication on the system of such vehicle and which is sold to a new owner). Conversely, the Data Holder would not know that the Data doesn't relate to the Initial User and would continue using / sharing the Data as contractually agreed with that user. Additionally, the Data Holder would not be able to ensure that the Data from the initial user was not accessible to other users. In such a case, other users and the Data Holder would have to rely on the initial User to ensure that they are properly informed and involved.

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

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

Access rights of the subsequent user may in particular depend on a contractual categorization of the Data, for instance:

(a) 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;

(b) Always Removable Data – Data which the Data Holder should not make accessible to the subsequent user;

(c) 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).

The Data Holder should sort the Data into these categories, particularly in the information referred to by Article 3 (2) and 3 (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 but 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**

10.1.1 Where the User contractually transfers (i) ownership of the Product, or (ii) their temporary rights to use the Product, and/or (ii) their rights to receive Related Services to a subsequent natural or legal person ('Subsequent User') and loses the status of a user after the transfer to a Subsequent User, the Parties undertake to comply with the requirements set out in this clause.

10.1.2 The User must:

*(if use of the Product and/or Service involves a new Contract between the Subsequent User and the Data Holder (for example, via creation of a new account)*

(a) ensure that the Subsequent User cannot use the initial User's account,

(b) notify the Data Holder of the transfer.

(*alternatively, if use of the product and/or related service does not involve a new Contract between the Subsequent User and the Data Holder*)

(a) use their best efforts to assign to the Subsequent User, as of the transfer date, their rights and obligations as a user and the Data Holder agrees hereby in advance to such assignment;

(b) without undue delay notify the Data Holder of the transfer and the identity of the Subsequent User and provide the Data Holder with a copy of the assignment; if absent an assignment under point (a), the User must without undue delay notify the Data Holder of the refusal, in which case the Data Holder may not use the Subsequent User's Data or make them available to third parties under clause 3.

10.1.3 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

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

10.2.2 The User must:

*(if the use of the Product and/or Related Service involves a new Contract between the Additional User and the Data Holder (for example, via creation of a new account)*

ensure that the Additional User cannot use the Initial User's account.

*(alternatively, if the use of the Product and/or Related Service does not involve a new Contract between the Additional User and the Data Holder)*

(a) include in the Contract between the User and the Additional User, as of the transfer date, on behalf of the Data Holder, provisions substantially reflecting the content of this contract and in particular clause 3 on the use and sharing of the Product and/or Related Service Data by the Data Holder ('Flow Down Provisions');

(b) act as a first contact point for the Additional User if the Additional User makes a request under Articles 4 or 5 of the Data Act or a claim regarding the use or making available of the Data by the Data Holder under this contract. The Data Holder should be notified of any request or claim in that regard without undue delay and the Parties must collaborate to address any request or claim.

### 10.3 Liability of the Initial User

If the User's failure to comply with their obligations under clauses 10.1 or 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 User will indemnify the Data Holder and hold them harmless in respect of any claims by the Subsequent or Additional User towards the Data Holder for the use of the Data after the transfer.

## 11 Date of application and duration of the Contract and Termination

### 11.1 Date of application and duration

This set of terms would usually not exist as a standalone contract, but rather be an ancillary contract to a main contract: either (i) a contract immediately executed such as a sale agreement for the connected product; or (ii) a contract successively executed such as lease or rental agreement for the connected product or service agreement for the related service.

In both cases, this Contract must generally remain into force as long as the main agreement 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 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] [unspecified time] [OPTION 2] [a fixed term of (specify)], unless it expires or is terminated in accordance with clauses 11.2 and 12.2.

**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 is otherwise put out of service or 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, with or without replacing this contract by a new contract.

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 13.3 on applicable law and clause 13.6 on dispute resolution, which remain in full force and effect.

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

(a) the Data Holder shall immediately 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) strict compliance with the obligation is of the essence of this Contract, in particular because non-compliance would cause significant harm to the other Party, the User or other protected third parties; or

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

(c) the non-performance is intentional.

12.1.2 A Party's non-performance is excused if it proves that it is due to an impediment beyond its control and that it 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 within a reasonable time after the non-performing Party knew or ought to have known of these circumstances. The other Party is entitled to damages for any loss 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 aggrieved Party shall have the remedies listed in the following clauses, without prejudice to any other 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 any of the remedies to the extent that its own act or state of affairs caused 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 for loss suffered to the extent that it could have reduced the loss by taking reasonable steps.

12.2.4 Each 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 unreasonable effort or expense;

(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 pecuniary damages caused to the aggrieved Party by the non-performance which is not excused under clause 12.1.2. The non-performing Party is liable only for damages which it foresaw or could reasonably 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.

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

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

(ii) *(if applicable)* provided that, where applicable, all other conditions set out in clause 5.4.3 are met.

12.2.6 The User can also:

(a) suspend the permission given to the Data Holder under clauses 3 or the limitations made under clause 8, until the Data Holder complies with their obligations, unless this would foreseeably cause a detriment to the Data Holder that is obviously disproportionate in the light of the seriousness of the non-performance;

(b) withdraw the permission given to the Data Holder under clauses 3 and/or their agreement to the limitations on User's rights agreed in 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 breach and the period has lapsed without the Data Holder remedying the breach. If the period stated is too short, the User may nevertheless terminate the Contract, but only after a reasonable period from the time of the notice.

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 loss resulting from the non-performance and the other circumstances.]

The Parties may wish to define penalties for defined types of non-performance as it may be excessively onerous for the Data Holder to prove the amount of actual damage caused by, e.g., failure to supply Data. Penalties must be proportionate.

## 13 General Provision

### 13.1 Confidentiality

13.1.1 The following information will be considered confidential information:

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

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

(c) information referring to the performance of this Contract and any disputes or other irregularities arising in the course of its performance;

(d) [OPTION] [the existence of this Contract and the identity of the Parties;

(e) [OPTION] [the terms and conditions of this Contract;].

13.1.2 Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 13.1.1. and not to disclose or make such information available to any third party unless one of the Parties

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

(b) has to disclose or make the relevant information available in order to fulfil its obligations under this Contract, and the other Party or the third party providing the confidential information or affected by its disclosure can reasonably be considered to have accepted this; or

(c) has obtained the prior written 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 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 Applicable law

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

### 13.4 Entire Contract, modifications and severability

13.4.1 This Contract (together with its appendices 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.

13.4.2 Any modification of this Contract shall be valid only if agreed to in writing, including in any electronic form that, in line with good commercial practices, is considered as fulfilling the requirements of a written document.

13.4.3 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 shall be unaffected by this and will continue to be valid and enforceable. Any resulting gaps or ambiguities in this Contract shall be dealt with according to clause 13.5**.**

### 13.5 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 EU law or national legislation adopted in accordance with EU law as well as any applicable national law that is compatible with EU 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 shall be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 13.3) and, in any case, according to the principle of good faith and fair dealing.

### 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 user's right 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] [For any dispute that cannot be settled in accordance with clause 13.6.1, the courts of (specify state) will, to the extent legally possible, have exclusive jurisdiction to hear the case.]

**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 data points

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).

## 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 classification

The appendix could 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 could 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 could 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 could 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. Means and information necessary for the exercise of the User's access rights

The appendix can specify here the means and 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: Form for an access request by the User**

This form is for one particular request. Multiple requests are possible under the Data Act 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).

| | |
|---|---|
| **Identification of the User** | Name: *Specify*<br>Contract n°: *Specify* |
| **Identification of the person making the request on behalf of the User (if applicable)** | Name: *Specify*<br>Relationship with the User: *Specify* |
| **Products and/or Services concerned by the request** | Product/Service 1: *Specify (e.g. serial number)*<br>Product/Service 2: *Specify (e.g. serial number)* |
| **Data concerned by the request** | ☐ All data which is readily available to the Data Holder<br>☐ Including personal Data<br>*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*<br>☐ After anonymization<br>☐ Only non-personal Data<br>☐ Other: *Specify* |
| **Date of Data concerned by the request** | ☐ Past data: *Specify the period*<br>☐ Future data: *Specify the period* |
| **Timing of access to the Data** *(depending on what is agreed in clause 4.3.2)* | ☐ Without undue delay<br>☐ Continuously<br>☐ Realtime<br>☐ With appropriate frequency<br>☐ Other: *please specify* |
| **Modalities for access to the Data** | ☐ Option 1 proposed by Data Holder<br>☐ Option 2 proposed by Data Holder |
| **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 the Data Act 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*<br>Contract n°: *Specify* |
| **Identification of the person making the request on behalf of the User (if applicable)** | Name: *Specify*<br>Relationship with the User: *Specify* |
| **Products and/or Services concerned by the request** | Product/Service 1: *Specify*<br>Product/Service 2: *Specify* |
| **Data concerned by the request**<br>**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<br>☐ 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*<br>☐ 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**<br>**Please note:** cannot be a gatekeeper under Article 3 of Regulation (EU) 2022/1925 | Name: *Specify*<br>Contact details: *Specify* |

**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)*

## ANNEX II: MODEL CONTRACTUAL TERMS
## for contracts between Users and Data Recipients

### 1. Parties and the Product/Related Services

### 1.1 Parties to the contract

This contract (the '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')

hereinafter referred to collectively as 'the Parties' and individually as 'the Party'.

**Parties**

'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 User's choice. It 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 Recipient may even be in competition with the relevant data holder. However, a gatekeeper is not eligible to become or be a Recipient.

**Scope**

The Model Contractual Terms ('MCTs') below aim to support the contractual relationship between the User and a third party of the User's choice and at the User's request, a Data Recipient, for data sharing in accordance with Article 5 of the Data Act, which states:

'*Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9.*'

These MCTs are aimed to govern the relationship between the User and the Data Recipient in respect of data (personal or non-personal). However, these MCTs do not deal with the underlying relationship between the parties that might be reflected in a main contract, for example: a contract for the development and/or provision of a service by the Data Recipient, etc.

These MCTs take into consideration Articles 7(2) and 13 of the Data Act (Unfair contractual terms unilaterally imposed on another enterprise). However, also as per EU and national law aspects regarding consumer protection, these MCTs do not include specific consumer protection clauses under applicable law. These should be included by the parties as necessary.

**1.2 Request to Data Holder and cooperation of the Parties**

1.2.1 The Parties agree that under the terms and conditions set forth in this contract,

[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.

1.2.2 The User and the Data Recipient will cooperate in good faith to arrange for the 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.

1.2.3 The request should be made and the H2R Contract should be concluded by [date]. If by [date], the request is not made, or the H2R Contract is not concluded, this Contract expires, or – subject to written agreement between Parties – such date to conclude the H2R Contract will be extended.

1.2.4 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 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 as the User under this Contract are set out in **Appendix 5**.

**2. Data covered by the Contract**

The data covered by the Contract consist of all readily available Product Data or Related Service(s) Data generated by the use of the Product or by Related Services, as identified under 1.2.4 above

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

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

[OPTION 3] within the meaning of the Data Act and that are necessary for purposes agreed under clauses 3 and further specified by the Data Recipient in **Appendix 2** of the H2R Contract.

The User expressly disclaims and waives all warranties regarding quality, characteristics and quantity of the Data and its 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 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.

'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 it 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, while still not limiting the Parties' use or re-use of the Data for other purposes than those listed in this contract.

### 3.1 Authorised use of the Data

It is up to the User to consider for what it would wish the Data Recipient to use (which part of) the Data and in particular whether and to what extent the Data Recipient should be allowed to share it with other third parties downstream – within scope of the defined purposes, for which the Data Recipient may use such Data.

The User may decide to specify one or more of specific use scenarios for the Data Recipient. Certain suggestions of potential use scenarios are listed in [OPTION 1] below.

For example, the User may request the Data Recipient to monitor the functioning of the Product or related Service and act as intermediary notifying warranty claims to the seller of the equipment on behalf of the User. However, the User may propose its own use scenario(s), also if currently not mentioned as one of the examples in [OPTION 1].

The User should also consider whether to allow the Recipient to share the Data, with commercial or non-commercial entities. The non-commercial data sharing may include altruistic or otherwise not-for-profit sharing and (re)use for public interest, scientific, statistical or other analytical research purposes (where applicable and required, respectively not-applicable or required but envisioned) in conformity to Article 89 GDPR, to the Open Data Directive (EU) 2019/1024, High Value Dataset Regulation (EU) 2023/138, Data Governance Act (EU) 2022/868, Health Data Spaces Regulation (EU) 2025/327, and the like), by or through the Data Recipient to 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 such relevant Data is otherwise handed over to the Data Recipient exclusively. This is neither needed or recommendable, also as Data is both a digital asset and a digital means, and can be used and re-used for many and multiple purposes throughout its life cycle – even multiple commercial purposes – while still granting a Data Recipient with market advantage or other value creation that for once also justifies a fair remuneration to the User for such license grant to (re)use the particular Data.

If the User does not have any specific use scenarios in mind, it may always allow the Data Recipient to use the Data for any purpose (see [OPTION 2]).

The User should assess the consequences of grating the Data Recipient the right to use, and if applicable, sharing the data and also consider whether such rights should be given against compensation.

Each of the options, and any combination thereof, should be non-exclusive, as per reasons mentioned above already: Data is both a digital asset and digital means, and can be used and re-used for many and multiple purposes throughout its life cycle. Therefore, it is recommended – regarding any purpose or combinations thereof – to avoid entering into any exclusive arrangements, except if such stipulations are well-scoped, data-specific-, market-specific, purpose-specific, time-limited and well-remunerated, while in no way limiting any other use or re-use of such Data for other purposes, markets and the like.

3.1.1 [OPTION 1] Subject to Union and national law on the protection of personal data, the Data Recipient undertakes to use the Data ("Use") only for the purposes agreed with the User as follows ("Authorised Purposes") (parties should specify the purpose, in particular they can choose one or more from listed below or describe their own purpose):

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

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

(c) improving the functioning of any product or related service offered by the Data Recipient;

(d) providing support, warranty, guarantee or similar services or to assess User's, Data Holder's, Data Recipient's or third party's claims related to the Product or Related Service;

(e) developing new products or services, including artificial intelligence (AI) solutions, by the Data Recipient, by third parties acting on behalf of the Data Recipient (i.e. where the Data Recipient 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);

(b) aggregating these Data with other data or creating of 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.

*(c) (other specific purposes agreed by the Parties as possible, to the extent those are not be in contradiction with the practices listed in clause 3.2).*

[OPTION 2] The Data recipient may use the Data for any purpose ("Authorised Purposes") other than the practices listed in clause 3.2.

3.1.2 The Data Recipient must erase the Data when the Data is no longer necessary 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 Authorises Purposes;

(b) for any purposes that are in violation of Union law or applicable national law, especially those designed to protect the User;

(c) for the profiling of natural persons within the meaning of Article 4(4) of the GDPR, notwithstanding Article 22(2) points (a) and (c) of the GDPR;

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

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

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

*(g)* 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 only use or otherwise process any Data that is personal data in full compliance with applicable data protection legislation (including but not limited to Regulation (EU) 2016/679).

| |
|---|
| In regulating the processing of personal data in accordance to the applicable data protection legislation (including but not limited to Regulation (EU) 2016/679), the parties shall consider whether: the User is the data subject of all personal data contained in the Data; The User is the data subject of some of the personal data contained in the Data; the User is not the data subject of the personal data contained in the Data. |

### 3.4 Application of protective measures

The Data Recipient undertakes to apply protective measures for the Data [OPTION 1] [as are reasonable in the circumstances, considering the state of science and technology, potential harm suffered by the User as a result of data loss or disclosure of data to unauthorised third parties and the costs associated with the protective measures.] [OPTION 2] [as set out in detail in **Appendix 2**, which forms an integral part of this Contract.]

Parties should consider whether they wish to include, in a separate Appendix, all the details of how important interests 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. Parties should be aware that the Data Holder or trade secret holder may request from Data Recipient to apply appropriate technical and organizational measures necessary to preserve confidentiality of shared data. If such measures are agreed they should prevail over the measures agreed between the Data Recipient and the User to avoid the situation that Data Recipient has to apply different protective measures or be in a breach of the Contract with ethe User.

## 4. Data sharing with third parties and data processing services

The User does not have to agree with the Data Recipient sharing the Data further, but can choose to give the Data Recipient this right. Thus, this clause should be inserted only if the User gives such rights to the Data Recipient, possibly against compensation.

### 4.1 Conditions for data sharing

4.1.1 The Data Recipient may share Data which is non-personal data with one or more third parties if:

(a) the third parties are identified in **Appendix 3** or the Data Recipient notified the User of the new third parties to be receiving the Data and the User has not objected to sharing the Data with them in accordance with clause 4.1.2 below; and
(b) the Data is used by the third party for the following purposes within the Authorised Purpose: [*specify the admissible purposes the third parties can pursue and whether the data is shared for these purposes against compensation]* (collectively: 'Admissible Subpurpose'); and
(c) the third party is not designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925 ('Data Markets Act'); and
(d) the Data Recipient contractually binds the third party
    (i) not to use the Data for any purposes than the Admissable Subpurpose;

    (ii) not to derive insights about the Data Holder's or the User's 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 protective measures required under Clause 3.4; and

(v) not to share these Data further unless the requirements set forth in Clause 4.1.2 are met or unless such data sharing is required, in the interest of the User, to fulfil this Contract or any contract between the third party and the User

(vi) to erase the Data when the Data is no longer necessary for the agreed purposes.

4.1.2 If the Data Recipient intends to share the Data with a third party not listed in Appendix 3, it should in a detailed manner notify the User in accordance with notification rules stated in Clause 9.5 before intended commencement of the sharing of its name, location and the Admissible Subpurpose. If the User does not object to such data sharing within 30 days after receipt of such notification, the Data Recipient may commence sharing the Data with such third party, subject to the terms in Clause 4.1.1.

The Data Recipient must oblige the third party with whom they share Data to include the clauses corresponding to Clause 4.1.1 (d) points (i) to (vi) in their contracts with further recipients.

[OPTION] Further details, including 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 The Data Recipient may, on its own risk and expense, also use services of data processing services providers to achieve the Authorised Purposes under Clause 3.1.

4.1.4 The Data Recipient shall only share with third parties or otherwise process any Data that is personal data in full compliance with applicable data protection legislation (including but not limited to Regulation (EU) 2016/679).

## 5. Compensation

> The Parties are free to discuss and agree on the compensation for sharing the data. Compensation may for instance (but is not required to) consist of remuneration (such as certain fees) but also, of providing certain services by the Data Recipient to the Use, in reduction of the fee charged by the Data Recipient for some services provided to the User, et cetera.

The Data Recipient undertakes to compensate the User as set out in detail in Appendix 4**,** for their Use of the Data in accordance with clause 3.1, including for sharing the Data with third parties in accordance with clause 4.1.

## 6. Fundamental declarations

### 6.1 Declarations of the Data Recipient

6.1.1 Data Recipient declares that they are not designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925 ('Data Markets Act').

6.1.2 The Data Recipient declares that any information provided to the User under this Contract is correct and accurate. The Recipient shall inform the User immediately of any material or other relevant changes in such information.

## 7. Duration of the Contract and Termination

> This set of MCTs could exist as a stand-alone contract, where data sharing is the main purpose of the contract. In that case, the Parties can use clauses 8 and 9 on Duration, Termination and Remedies.
>
> Data sharing can also be ancillary to a main contract, e.g. a contract for repair and maintenance of an industrial machine. In that case, the clauses on Duration, Termination and Remedies of the main contract should usually be sufficient, and the clauses 8 and 9 of these MCTs would not be needed.

### 7.1 Duration and termination

7.1.1 This Contract [OPTION 1] is made for the period of [insert period], [OPTION 2] comes into effect on [insert date] and is concluded for an indeterminate period, subject to any grounds for termination under this Contract.

7.1.2 The Data Recipient will terminate this Contract by giving notice within [notice period] to the User if the H2R Contract has been terminated.

7.1.3 If the User loses their status as a User, this Contract will terminate. The User will give notice within [notice period] to the Data Recipient.

7.1.4 [OPTION in case of indeterminate period or if the Parties wish to allow termination for convenience] Either Party may terminate the Contract at any time before the start of or during the contract period by giving [insert period] notice to the other Party.

> 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.

7.1.5 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) 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 [time]]; if the Data Recipient does not intend to use or share such Data after termination or expiry, they should delete the Data, no later than [60] days after termination/expiry and should notify the User that they have done so.

(c) [OPTION] If the User terminates the Contract under clause 7.1.4 before *[insert point in time or minimum contract period]* the User shall compensate the other Party

for the investment made in relation to the implementation of this Contract, as follows: [*specify as appropriate*]

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

## 8. Remedies for breach of Contract

### 8.1 Remedies and non-performance

8.1.1 The rights and remedies provided under this Contract in case of breach are in addition to, and not exclusive of, any rights or remedies provided by law. Remedies which are not incompatible may be cumulated. In particular, the aggrieved Party is entitled to claim damages in addition to the exercise of any other remedy.

8.1.2 A non-performance of an obligation amounts to a fundamental breach to this Contract if:

(a) strict compliance with the obligation is of the essence of this Contract, in particular because non-compliance would cause significant harm to the other Party, or other protected third parties; or

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

(c) the non-performance is intentional and gives the aggrieved Party reason to believe that it cannot rely on the other Party's future performance.

8.1.3 A Party’s non-performance is excused if it proves that it is due to an impediment beyond its control and that it 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 within a reasonable time after the non-performing Party knew or ought to have known of these circumstances. The other Party is entitled to damages for any loss resulting from the non-receipt of such notice.

8.1.4 Remedies for breach:

In the event that any Party fails to comply with its obligations under this Contract, the other Party shall have the following remedies:

(a) Right to Terminate: Each Party shall have the right to immediately terminate this Contract, without penalty, if

(i) the other Party's non-performance is a fundamental breach,

(ii) if the other Party breaches any material obligation and fails to remedy such breach within [30] days of receiving written notice of such breach

(b) Damages for breach: The aggrieved Party is entitled to damages for any pecuniary loss, damage, or injury suffered due to a breach of the Contract which is not excused under clause 8.1.3, including but not limited to a breach concerning use or provision of the data, loss of personal data, unauthorized access, or misuse of data, caused by the other Party's non-performance.

The non-performing Party is liable only for loss which it foresaw or could reasonably 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.

The amount of damages shall be based on the actual loss suffered by the aggrieved Party, including any consequential and incidental damages, to the extent permitted by law. [This amount shall not exceed EUR [*].]

(c) Specific Performance: In the case where a Party fails to perform its obligations other than a monetary performance, the aggrieved Party may request that the non-performing Party comply, without undue delay, with its obligations under this Contract. The aggrieved Party may apply to court for an order for specific performance of the Contract if permitted by applicable law.

Specific performance cannot, however, be obtained where:

(i) performance would be unlawful or impossible; or

(ii) performance would cause the other Party unreasonable effort or expense; or

(iii) the performance consists in the provision of services or work of a personal character or depends upon a personal relationship, or

(iv) the aggrieved Party may reasonably obtain performance from another source.

8.1.5 [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 6**, which the Parties deem damages within the meaning of clause 8.1.4 (b). 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 loss resulting from the non-performance and the other circumstances.]

## 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 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;

(d) [OPTION] the existence of this Contract and the identity of the Parties;

(e) [OPTION] the terms and conditions of this Contract;

(f) information referring to the performance of this Contract and any disputes or other irregularities arising in the course of its performance.

9.1.2 Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 9.1.1. and not to disclose or make available such information to any third party, unless one of the Parties:

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

(b) has to disclose or make available the relevant information to meet its obligations under this Contract, and the other Party (or the party providing the confidential information or affected by its disclosure) can reasonably be considered to have accepted this; or

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

9.1.3 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 1.2.2.

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 EU or Member State law.

**9.2 Applicable law**

This Contract is governed by the law of [*specify state]*

**9.3 Entire Contract, modifications and severability**

9.3.1 This Contract (together with its appendices and any other documents referred to in the Contract) 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.

9.3.2 Any modification of this Contract will be valid only if agreed to by the Parties in writing, including in any electronic form that is considered to meet the requirements of a written document (in line with good commercial practices).

9.3.3 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 according to clause 9.4.

### 9.4 Interpretation

9.4.1 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 EU law or national legislation adopted in accordance with EU law, as well as any applicable national law that is compatible with EU law and cannot be derogated from by agreement.

9.4.2 If any gap or ambiguity in this Contract cannot be resolved in the way referred to in clause 9.4.1 this Contract must be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 9.2) and, in any case, according to the principle of good faith and fair dealing.

### 9.5 Notifications

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.

### 9.6 Dispute settlement

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 competences 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]*.

**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 III: 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

### 1. Parties, Requesting User and subject matter

### 1.1 Parties to the Contract

This contract on the access to and use of data ('the Contract) 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 document 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 holder' 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.

### 1.2 Requesting User, Product and 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) 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 services or type of related services covered by the Contract, if applicable).*

> The Parties must identify here:

(i) who is the user within the meaning of Article 2(12) of the Data Act,

(ii) 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.

They 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) which 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 Fundamental declarations

### 2.1 Quality of the 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 specified in 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 provided evidence that they have 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 themself.

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 to an even greater extent than 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 further declares that, to the best of their knowledge, the request is valid under applicable law, has not been withdrawn and has not expired. In particular, the Data Recipient

declares that it has not made the exercise of choices or rights under the Data Act by the Requesting User unduly difficult, including by offering choices to the Requesting User in a non-neutral manner, or by coercing, deceiving or manipulating the Requesting User, or by impairing the autonomy, decision-making or choices of the Requesting User, including by means of a user digital interface or a part thereof.

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 should:

- qualify as a freely given, sufficiently informed and explicit indication of the Requesting User's wishes (which is not the case, in particular, where the Requesting User has been encouraged to make a request by deceptive or coercive means or by subverting or impairing their autonomy );
- be given with the legal capacity required under the applicable laws, including, for personal data, EU and national data protection laws; and
- not be invalid on other grounds.

## 2.2 Eligibility of Data Recipient

2.2.1 The Data Recipient declares that they have entered into an contract with the Requesting User on the use of the Data. 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 is strictly necessary for fulfilling this purpose.

The Parties should endeavour to define the purpose in a way that allows the Data Holder to determine whether the use of the data by the Data Recipient is permissible and to apply technical and organisational safeguards to ensure that it is; 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 is does not qualify as a undertaking designated as a 'gatekeeper' under 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 the 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 captures any data that relates 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 allows to link the data to identified or identifiable individual. This can happen also 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 is disclosed, whether a third party or not (not including public authorities, who may receive personal data in the framework of a particular inquiry under the applicable law).
>
> The Parties should consider that a party may have more than one role depending of the processing purpose, and/or may have a role jointly with another party.
>
> When the Requesting User is not the data subject, a legal basis is needed under GDPR to allow the sharing of the Data with the Data Recipient. A possible legal basis could be consent within the meaning of Article 6 (1) (a) or the 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 Incorrectness of fundamental 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, correct, or will no longer remain correct 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).

2.4.2 On becoming aware of this situation, each of the Parties must take appropriate action and cure the false or incorrect fundamental 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 the temporary suspension of the making available of the Data 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 is or has become unlawful.

> If any declaration referred to in clauses 2.1 to 2.3 is not or no longer correct, the party should undertake appropriate actions. 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 it should indicate the reason of termination. The mere notification would not be sufficient in this case, as there is no way to rectify the situation. If the Data Recipient wants 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 for example the case when the user's request is issued by unauthorised person (e.g. the employee who had no power to represent the user company). In such case, the local law may allow to validate such action with retroactive effect by the Management Board of the user.

2.4.3 If the situation is not and cannot be cured, this Contract must terminate by means of a written termination notice mentioning the reasons of termination given by either party to the other. The termination has immediate effect. Where the incorrectness 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 on the basis of Article 5 of the Data Act, as well as the relevant metadata necessary to interpret and use that data ('the Data').

3.1.2 The Data is set out in detail in **appendix 2**, which forms an integral part of this Contract.

> The Parties should, in a separate appendix, specify the data 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 Services 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**, i.e. 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** that the Data Holder can lawfully obtain from the product or related service, without disproportionate effort going beyond a simple operation.

As this Contract defines the arrangements for making the Data available to the Data Recipient at the request of the Requesting User, this Data is that identified in the request.

The Data must also include, in accordance with Article 5 (1) of the Data Act, the relevant metadata necessary to interpret and use the data.

The description of the Data must be sufficient to determine which data is covered by a specific regime, if any. In particular, the Parties must set out the details regarding which of the Data qualifies as personal data.

### 3.2 Data quality and access arrangements

3.2.1 The Data Holder must make the Data available to the Data Recipient, with at least the same quality as it becomes 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.

3.2.2 The Data Recipient must receive access to the Data

(a) easily and securely, either [OPTION 1] [by the data being transmitted] [OPTION 2] [by access to the Data where it is stored];

*(if applicable)* (b) without undue delay after the Data becomes available to the Data Holder;

*(if applicable)* (c) [OPTION 1] [continuously and in real-time] [OPTION 2] [with appropriate frequency].

3.2.3 The Data Holder must provide to the Data Recipient the means and information strictly 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.

3.2.4 In order to meet the requirements of clauses 3.2.1, 3.2.2 and 3.2.3, the Parties agree on the specifications set out in **Appendix 2**, which forms an integral part of this Contract.

3.2.5 If any of the specifications concerning data quality, access arrangements or means and information provided to the Data Recipient are insufficient to meet the requirements referred

to in clauses 3.2.1, 3.2.2 and 3.2.3, the Parties undertake to enter into negotiations in good faith and adapt the specifications so that they meet the agreed requirements.

Parties should agree on all the details of how access is to be provided.

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 is 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 it is stored**, i.e. the Data is 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 is not transferred to a medium within the Data Recipient's control.

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

Access where the data is 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 where the data is stored, there are further technical possibilities, including access on the Requesting User's device.

If Parties go for access where the Data is stored, there are a number of details to solve, including how to make sure that the Data Recipient's business ideas are not disclosed and which 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 where the data is 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 where the data is 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 where the Data is 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. According to 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 access is provided in real time, and if not during which periods.

In addition to the basic questions of full transfer or access where the data is stored, and the timing of access, the Parties must consider a range of further issues, such as which access credentials are required, and which and how many employees of the Data Recipient may access the Data.

Last, the Data Holder must provide for free the means and information strictly necessary for the exercise of the right to access Data in accordance with article 4. This could also be specified 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 quality and access arrangements and if the Data Recipient notifies 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 of the incident. If the incident was caused by a failure of the Data Holder to comply with their obligations, they must remedy the breach [OPTION 1] [within a reasonable period of time] [OPTION 2] [within a time period of (specify)]. If the Data Holder does not do so, it is considered as a fundamental breach and the Data Recipient is entitled to invoke clauses 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 unreasonable to achieve because of a change of circumstances, the Data Holder must notify 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 defined in these clauses. In particular, each Party must provide to 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 clauses 8.

### 3.4 Unilateral changes by the Data Holder

3.4.1 The Data Holder may, in good faith, unilaterally change details regarding the specifications for the Data and access arrangements, if this is objectively justified by the general 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 the clauses 3.2.

3.4.2 The Data Holder must in this case give notice of the change to the Data Recipient [OPTION 1] [without undue delay] [OPTION 2] [within (*specify a reasonable period of time*)] after deciding on the change. Where the change may negatively affect data access and use by the Data Recipient, the Data Holder must give notice to the Data Recipient at least (indicate a

reasonable period of time longer than the period in the first sentence) before the change takes effect.

A shorter notice period may only suffice 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 has detrimental impact on 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)* 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 is considered to be protected as a trade secret, as this would subvert the intended effects of the Data Act.

   *See clauses 4.1.1, 4.1.2, 4.1.3, 4.1.4 and 4.4.1.*

2. **Trade secrets** – However, if the Data Holder identifies that certain Data covered by this Contract are protected as trade secrets, they are entitled to certain rights, primarily to continue to preserve the confidentiality of the secrets in question by implementing reasonable steps as provided for by the Trade Secrets Directive (EU) 2016/943.

   To see which Data is protected as a trade secret and how to define a 'trade secret holder', see Article 2(1) of the Trade Secrets Directive.

   *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 is identified in the Contract. The data holder must therefore inform the data recipient prior to concluding the Contract with the data recipient.

   *If yes, see clause 4.1.2 and the other clauses hereunder cater for that.*

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.

   *For such cases, clause 4.1.3 and the other clauses hereunder cater for that.*

5. **Audit rights -** In order to preserve the confidentiality of the Data protected as trade secrets, while not interfering with each other's activities, certain audit rights by means of involving independent third parties are to be considered, including mechanisms in 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, 4.3 and the trade secret appendix.*

7. **Trade secret holder rights (2/4)** – if the initial measures do not suffice, the trade secrets 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 secrets 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 suspend data sharing in accordance with clauses 5.4.2, 5.4.3 or 5.4.4, the Data Holder will still be obliged to keep the related Data containing Identified Trade Secret readily available by retaining it up to the moment that it can be shared within scope of the Contract.

    *See clause 4.5.*

11. **Third party identified trade secret holder** – if the trade secrets 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 secrets 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 shared by the Data Holder with 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 said Directive).

4.1.2 The data protected as trade secrets (hereafter these will be referred to as 'Identified Trade Secrets') and the identity of the Trade Secret Holder(s) are set out **Appendix 4**, which forms an integral part of this Contract.

The Data Holder herewith declares to the Data Recipient that they have all relevant authorisations and other rights of the third party Identified Trade Secrets holders to enter into this Contract regarding the applicable Identified Trade Secrets and all the related rights and obligations under this Contract.

According to Article 2(1) of the Trade Secret Directive, the term '**Trade Secret**' means information which meets all of the following three (3) 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 protected as Trade Secrets if the Data Holder or the Trade Secret Holder took such steps before from any request made in accordance with article 5 of the Data Act.

4.1.3 If, during this Contract, new data are made available to the Data Recipient that is 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 the Trade Secret Appendix has been amended and agreed between the Parties, the Data Holder may temporarily suspend the sharing of the specific newly Identified Trade Secret(s) by giving notice to the Data Recipient and the competent authority designated under Article 37 of the Data Act, with a copy of this sent to the Data Recipient.

4.1.4 The declarations and 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 **Appendix 4** (hereafter these are referred to as '*Identified Trade Secrets DR Measures*').

Parties should, in a separate appendix, which forms part of the Contract, include all the details of these measures. Measures may be both technical (e.g. encryption, firewalls, split storage, etc.) and organisational (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(s). The measures will also depend on whether (i) access is to be provided where the data is stored or (ii) the data is 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 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 to make Data protected as trade secrets available to a third party, the Data Recipient must inform the Data Holder of the fact that Identified Trade Secrets have been or will be made available to a third party, specify the data in question, and give the Data Holder the identity and contact details of the third party.

4.2.3 [OPTION] [In order to verify if and to what extent the Data Recipient has implemented and is maintaining the Identified Trade Secrets DR Measures, the Data Recipient agrees to either (i) annually obtain, at Data Recipient's expense, a security conformity assessment audit report from an independent third party chosen by the Data Recipient, or (ii) to annually allow, at 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 Data Recipient. Such security audit report must demonstrate Data Recipient's compliance with availability, integrity, confidentiality principles

as further described in the Trade Secrets Appendix 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 the Data Recipient opts for a security audit from an independent third party at Data Holder's expense as set forth above, it retains the right to obtain security audit report from an independent third party at Data Recipient's expense if it deems the security audit report from an independent third party at Data Holder's expense is not correct. If this right is exercised, both independent third-party auditors, together with Parties, will discuss any difference between those two reports and aim to resolve any pending materials matters while observing good faith.]

**4.3 Protective measures taken by the Data Holder**

4.3.1 The Data Holder may apply the measures set out in detail in **appendix 4** to preserve the confidentiality of the shared and otherwise disclosed Identified Trade Secrets (hereafter these are referred to as '*Identified Trade Secrets DH Measures*'.

4.3.2 The Data Holder may also add unilaterally appropriate technical and organisational protection measures, if they do not negatively affect the access to and use of the Data by the Data Recipient under this Contract.

4.3.3 The Data Recipient undertakes not to alter or remove such Identified Trade Secrets DH Measures unless otherwise agreed by the Parties.

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

4.4.1 The Data Holder must share the Data with the Data Recipient, including Identified Trade Secrets, in accordance with this Contract and must not refuse, withhold or terminate the sharing of any Identified Trade Secrets, except as explicitly set forth in clauses 4.4.2, 4.4.3 and 4.4.4 respectively.

4.4.2 Where the Identified Trade Secrets DR Measures and the Identified Trade Secrets DH Measures do not materially suffice to adequately protect a particular Identified Trade Secret, the Data Holder may, by giving notice to the Data Recipient with a detailed description of the inadequacy of the measures:

(a) unilaterally increase their Identified Trade Secrets DH Measures regarding the specific Identified Trade Secret in question, providing this increase is compatible with their obligations under this Contract and does not negatively affect the Data Recipient, or

(b) 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 of such measures is duly substantiated, e.g. in a security audit report, the Data Holder may suspend the sharing of the specific Identified Trade Secret by giving notice to the Data Recipient and the competent authority designated under Article 37 of the Data Act, with a copy of this sent to the Data Recipient.

The Data Holder must continue to share any Identified Trade Secrets other than these specific Identified Trade Secrets and is not entitled to terminate the Contract.

4.4.3 If, in exceptional circumstances, the Data Holder is able to demonstrate that they are highly likely to suffer serious economic damage from disclosure of a particular Identified Trade

Secret to the Data Recipient despite the Identified Trade Secrets DR Measures and, if applicable, the Identified Trade Secrets DH Measures having been implemented, the Data Holder may stop sharing the specific Identified Trade Secret in question.

They may do this only if they give duly substantiated notice to the Data Recipient and the competent authority designated under Article 37 of the Data Act (with a copy being sent to the Data Recipient).

However, the Data Holder must continue to share any Identified Trade Secrets other than those specific Identified Trade Secrets.

| |
|---|
| 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 e.g. the lack of enforceability of trade secrets protection in non-EU countries, the nature and level of confidentiality of the Identified Trade Secret in question or the uniqueness and novelty of the relevant connected product. |

4.4.4 If the Data Recipient fails to implement and maintain their Identified Trade Secrets DR Measures and if this failure is duly substantiated by the Data Holder e.g. in a security audit report from an independent third party, the Data Holder is entitled to withhold or suspend the sharing of the specific Identified Trade Secrets, until the Data Recipient has resolved the issue as described in the following two paragraphs.

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

On receiving this notice, the Data Recipient must address the issue without undue delay (i.e. they must (i) assign the appropriate priority level to the issue, based on its potential detrimental impact and (ii) resolve the issue in consultation with the Data Holder and otherwise in accordance with the applicable proceedings set out in the trade secrets appendix).

4.4.5 Clause 4.4.2 does not entitle the Data Holder to terminate the Contract. Clauses 4.4.3 or 4.4.4 entitle the Data Holder to terminate the Contract only with regard to the specific Identified Trade Secrets, and if (i) all the conditions of clause 4.4.3 or clause 4.4.4 have been met, (ii) no resolution has been found by Parties after *(insert 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 (iii) the Data Recipient has not been awarded by a competent court with 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, suspend or in any other way end or refuse the data sharing to the Data Recipient in accordance with clauses 4.4.2, 4.4.3 and 4.4.4, it will need to ensure that the particular Data that is the subject matter of the exercising of such right is retained, so that said Data will be made available to the Data Recipient:

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

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

Above 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 4.4.5.

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 in part or in full where and to the extent the withholding, suspension or refusal to provide data was caused by the Data Recipient acting in bad faith.

## 5 Use of the Data and sharing with third parties

### 5.1 Permissible use by 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 it 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 technical and organisational 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 clause 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 and that the third party is liable towards the Data Holder for any harm caused by such unauthorised use or disclosure of the data.

5.2.3 The Data Holder may always 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 the agreed purposes under clause 5.1.

**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 protective technical or organisational measures agreed under clause 4.2; or

(c) alter or remove, without the agreement of the Data Holder, any protective measures applied by the Data Holder under clause 4.3; 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;

(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) notwithstanding Article 22 (2) points (a) and (c) of the GDPR, 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 The Data Recipient must comply, without undue delay, with requests by the Data Holder, the holder of the relevant trade secret (if this is not the same as 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 this data, or the importation, export or storage of infringing goods for those purposes;

(e) destroy any infringing goods, if 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 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

### *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 declares 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**].

> The Parties should, in the Contract itself or in a separate appendix, determine details on compensation.
>
> They should agree, at least, on the following:
>
> - the amount of compensation due, and the currency;
> - the time when payment is due; and
> - the arrangements for payment.

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 of data collection or production.

[OPTION] [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, clause 4.5 shall apply accordingly.

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 Data Recipient declares that they do not qualify as a micro, small or medium enterprise (SME) under Recommendation 2003/361/EC. The Data Recipient is aware that, if they meet the qualifications to be classed as an SME at some point in the future, this may influence the compensation due under this Contract.

In this case, it is the responsibility of the Data Recipient to inform the Data Holder and to provide evidence that they meet the criteria relevant for being an SME.

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

> 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.
>
> The Data Holder must 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.

6.2.3 The Parties confirm that they consider the agreed compensation to be non-discriminatory and reasonable.

The Data Holder further confirms that the amount does not go beyond:

(a) the costs incurred for making the data available, including, in particular, the costs necessary for formatting the data, disseminating it via electronic means and storing it;

(b) the investment in the collection and production of data, where applicable, taking into account whether other parties contributed to the obtaining, generating or collecting of the data in question; and

(c) a margin.

[OPTION] [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**.]

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

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

### 7.1 Date of application and duration

7.1.1 This Contract [OPTION 1] [comes into effect on *(specify date)*] [OPTION 2] [comes into effect on *(specify date) and* is made for the period of *(specify period)*] [OPTION 3] [comes into effect on *(insert date)* and is concluded for an indeterminate period], 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 in clause 8.1.
>
> 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 8.2, depending on whether the Requesting User has specified a particular time period.

7.1.2 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 not necessarily so, in particular not if one or both Parties still 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 is otherwise put out of service or loses its capacity to generate the Data in an irreversible manner; or

(b) when both Parties so agree, with or without replacing this Contract by a new Contract.

7.2.2 The Data Recipient may terminate the Contract at any time 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 9.3 on applicable law and clause 9.7 on dispute resolution.

7.3.2 On termination of this Contract a Party may recover money paid for a performance which they did not receive or which they properly rejected.

A Party that has rendered performance which can be returned and for which they have not received payment or other counter-performance may recover the performance.

A Party that has rendered a performance which cannot be returned and for which they have not received payment or other counter-performance may recover a reasonable amount for the value of the performance to the other Party.

7.3.3 The Parties must take appropriate and reasonable steps to prepare for expiry of the contract period or termination of this Contract. [OPTION 1] [This may, depending on the circumstances, include such exit support measures as the Data Recipient may reasonably expect.] [OPTION 2] [This includes 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 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, 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 to this Contract if:

(a) strict compliance with the obligation is of the essence of this Contract, in particular because non-compliance would cause significant harm to the other Party, the Requesting User or other protected third parties; or

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

(c) the non-performance is intentional.

8.1.2 A Party's non-performance is excused if the non-performing Party proves that it is due to an impediment beyond its control and that it 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 within a reasonable time after the non-performing Party knew or ought to have known of these circumstances. The other Party is entitled to damages for any loss resulting from the non-receipt of such notice.

### 8.2 Remedies for breach of contract

8.2.1 In the case of a non-performance by a Party the aggrieved Party shall have the remedies listed in the following clauses, without prejudice to any other 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 any of the remedies to the extent that its own act or state of affairs caused 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 for loss suffered to the extent that it could have reduced the loss by taking reasonable steps.

8.2.4 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 unreasonable effort or expense;

(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, where applicable, all conditions set out in clause 4.4.4 are met];

(c) terminate the contract with immediate effect if:

(i) the non-performance is fundamental; or

(ii) in the case of non-performance which is not fundamental, the aggrieved Party has given a notice fixing a reasonable period of time and the period has lapsed without the other Party remedying the breach. If the period stated is too short, the aggrieved Party may nevertheless terminate the Contract, but only after a reasonable period from the time of the notice;

*(if applicable)* [provided that, where applicable, all conditions set out in clause 4.4.5 are met;]

(d) claim damages for pecuniary loss caused to the aggrieved Party by the non-performance which is not excused under clause 8.1.2. The non-performing Party is liable only for loss which it foresaw or could reasonably 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.

8.2.5 [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 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 where it can prove that the penalty is grossly

excessive in relation to the loss resulting from the non-performance and the other circumstances.

| |
|---|
| The Parties may wish to define penalties for defined types of non-performance as it may be excessively onerous for the Data Holder to prove the amount of actual damage caused by, e.g., failure to supply Data. Penalties must 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 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 the Requesting User and any other protected third party, unless the protected third party has made this information public;

(d) information referring to the performance of this Contract and any disputes or other irregularities arising in the course of its performance;

(e) [OPTION] [the existence of this Contract and the identity of the Parties;]

(f) [OPTION] the terms and conditions of this Contract].

9.1.2 Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 9.1.1 and not to disclose or make available such information to any third party, unless one of the Parties:

(a) has a legal right or is under a legal obligation to disclose or 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) has to disclose or make available the relevant information to meet its obligations under this Contract, and the other Party (or the party providing the confidential information or affected by its disclosure) can reasonably be considered to have accepted this; or

(c) has obtained the prior written 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 its 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 EU or Member State law.

**9.2 Non-discrimination**

The Data Holder declares that – with the terms of this Contract and any practices related to its fulfilment – when making data available, they 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.

If the Data Recipient considers the conditions under which data has been made available to them to be discriminatory, the Data Holder must, on request by the Data Recipient, demonstrate that there has been no discrimination.

**9.3 Applicable law**

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

**9.4 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.

**9.5 Entire Contract, modifications and severability**

9.5.1 This Contract (together with its appendices and any other documents 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.

9.5.2 Any modification of this Contract will be valid only if agreed to by the Parties in writing, including in any electronic form that is considered to meet the requirements of a written document (in line with good commercial practices).

9.5.3 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. Any resulting gaps or ambiguities in this Contract must be dealt with according to clause 9.6.

**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 EU law or national legislation adopted in accordance with EU law, as well as any applicable national law that is compatible with EU 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 9.3) and, in any case, according to the principle of good faith and fair dealing.

**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 Submission of a dispute to a dispute settlement body according to clause 9.7.1 does not, however, affect the right of the Data Recipient to lodge a complaint with the national competent authority designated in accordance with the Data Act; nor the right of any Party to seek an effective remedy before a court or tribunal in a Member State.

9.7.3 [OPTION, if the User is a business] [For any dispute that cannot be settled according to clause 9.7.1, the courts of *(specify state)* will, to the extent legally possible, have exclusive jurisdiction to hear the case.]

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

**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 contains a mere 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 to their needs. The Parties can in particular add to this list.

## A. Specification of data points

The Appendix should 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.

## 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 points or group of data points.

## C. Classification / Data Type

The appendix could 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. Transfer/Access Medium

The appendix should specify here via which secure-convenient electronic medium will the Data be made available by Data Holder to Data Recipient, either by transfer, access or otherwise, while catering for the rights and related due interests of Data Recipient under the Contract.

## F. Timing to Access of Data

The appendix should specify what is the rate, frequency, and other time-related parameter 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. Means and information necessary for the exercise of the Data Recipient's access rights

The appendix can specify here the means and 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 Data Recipient's side.

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

## Appendix 4 (Trade Secrets)

In this Appendix that is an integral part of the Contract, Parties should include all the operational, organisational and contractual details as deemed necessary for the protection of Identified Trade Secrets. This can include the elements listed below.

In any case, this (i) shall not be at a higher level than how the Identified Trade Secrets Holder itself preserves the confidentiality of the Identified Trade Secrets and (ii) should cater for the rights and related due interests of Data Recipient under the Contract and by law (in particular the Data Act) as well.

### A. Identified Trade Secrets Holder(s)

The appendix should identify who is or are the Identified Trade Secrets Holder(s).

### B. Identified Trade Secrets

The appendix should identify the data points protected as trade secrets.

### C. Security

The appendix should specify how the Identified Trade Secrets will be secured, while catering for the rights and related interests of Data Recipient under the Contract.

Special attention and consideration should be given to:

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 system, portal, platform and related Application Programming Interfaces (APIs) and the like;
vii. Data Holder-side security;
viii. provision and assurance of the Data Recipient side;
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. Continuous assurance monitoring and incident handling policies and capabilities.

**D. Transfer/Access Medium**

The appendix could specify special arrangements related to the means of transfer of or access to the Data.

**E. Secure Use**

The appendix should specify here in what common secure manner the Data Recipient can use the Identified Trade Secrets.

**F. Identified Trade Secrets DH Measures**

The appendix should specify the appropriate technical and organisational protection measures implemented during the Contract by the Data Holder to preserve the confidentiality of the Identified Trade Secrets ('*Identified Trade Secrets DH Measures*').

**G. Identified Trade Secrets DR Measures**

The appendix should specify the appropriate technical and organisational protection measures to be implemented during the Contract by the Data Recipient to preserve the confidentiality of the Identified Trade Secrets ('*Identified Trade Secrets DR Measures*').

**H. Accountability**

The appendix should specify the accountability tools, procedures or methodologies the Data Recipient can demonstrate continuous compliance their obligations related to the Identified Trade Secrets, to the extent not already stated in the Contract and not conflicting with terms thereof.

**I. Key Contact Details**

The appendix should identify who is the key contact person(s) in the Data Holder's and Data Recipient's side, including technical contact person(s).

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

### 1. Parties

This contract (the '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')

hereinafter referred to collectively as 'the Parties' and individually as 'the Party'.

**Scope**
This Contract only applies where the data sharing is purely voluntary between Data Sharer and Data Recipient, i.e. Data Sharer is not obliged to share data in accordance with the Data Act or in accordance with any other legal obligation contained in EU or national law (such as Articles 6(9) and 6(10) of the Digital Market Act).
In cases of mandatory data sharing of product data and related services 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 scenario) 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 scenario).
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 article 8 of the Data Act are complied with. Dedicated sets of terms developed by the European Commission, or a Member State may apply to such mandatory data sharing scenario.
In all cases of voluntary data sharing between enterprises, Chapter IV (Article 13) of the Data Act shall apply as the Data Act seeks to ensure fair data sharing agreements for the overall target to create a balanced single market of data. Chapter IV goes beyond data access and use of IoT data and applies – in fact - to any clause on access and use of data as broadly defined by the Data Act. Chapter IV therefore applies to all data sharing agreements between enterprises.

**Parties**
The parties to this Contract are business entities, i.e. the Data Sharer and the Data Recipient.

1. Data Sharer can be any business entity 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 MCTs (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 existence of a legal basis).
Data Act related use-cases, when the Data Sharer could be:

- A Data Holder under article 2(13) of the Data Act, who has the right to share product data and related service data, or who wants to share derived or inferred data

- A User of a connected product or related service to whom data was 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 the Data Act, who now has the right to use and make available data in accordance with its agreements with the user and Data Holder

Other use-cases, when the Data Sharer could be:

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

2. Data Recipient can be any business entity to whom 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 ('the Data') consists of the Data identified in **Appendix 1**, as well as the relevant metadata necessary to interpret and use those 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), Data Sharer commits to identify such Data in **Appendix 2**, as well as to take 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 is not shared, it does not need to be listed in **Appendix 2**; if it is shared however, it must be listed and protected accordingly.
Data identified as such in **Appendix 2** may for example be:

- protected as a trade secret by Data Sharer in which case it will be covered under the clause on "Trade Secrets";
- considered as confidential by Data Sharer in which case it will be protected under clause "Confidentiality";
- protected by the sui generis database rights or any other intellectual property rights, in which case clause "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.

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 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 which case this set of terms can be used.

## 3. Fundamental declarations

### 3.1 Origin of the data

3.1.1 Data Sharer hereby declares that Data provided under this Contract originates from the following sources: [Please insert all sources of Data and specify, 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 like demographic data inputted 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 CRM 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 Recipient being unable to verify the legality of such Data and its origin. The Recipient therefore needs to rely on the Sharer and may wish to obtain certain warranties in that regard. However, warranties may not be relevant in the situation where the 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 a SME and/or that the Data is retrieved directly from the Product.

3.1.2 The Data Sharer warrants that:

(i) *(If applicable:)* Where the Data contains non-personal Product or Related Services Data (as defined by the Data Act) and the Data Sharer under this Contract has access to the data in its quality 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 sharing of the Data for the purposes contemplated under this Contract;

(ii) *(If applicable:)* Where the Data contains Product or Related Services Data and the Data Sharer under this Contract has gained access to it in accordance with Article 4 of the Data Act in its role as a User, this Contract reflects the contractual commitments taken with the Data Holder and does not aim at:

a. developing a connected product that competes with the product from which the Data originates;

b. sharing the Data with a third-party considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925.

(iii) *(If applicable:)* Where the Data contains Product or Related Services Data and the Data Sharer under this Contract has gained access to it in its quality as a Recipient under Article 5 of the Data Act, this Contract is not in breach of contractual commitments with the User and Data Holder and obligations under the Data Act (including points a and b of 3.1.2 (ii)).

(iv) 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;

(v) except as otherwise specified in **Appendix 2** and without prejudice to Clause 3.2, it has obtained and will maintain for the duration and purpose of the Contract, at its own cost, all permissions, licenses and authorizations required for sharing and use by Data Recipient of any Data obtained from or provided by a third party. The Parties shall discuss and agree in good faith on the costs for obtaining such permission, licenses or authorizations.

3.1.3 [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.

3.1.4 [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 [choose: professional-, ethical industry-, cybersecurity-, research- and AI-] standards.

3.1.5 [OPTION] Where the parties to this Contract use a data intermediation service according to Article 2 (11) of the Data Governance Act to facilitate the data sharing, the Party which entered into the agreement with such data intermediation service has taken appropriate measures to verify that the data intermediation service is recognized as such in the Union.

### 3.2 Compliance with data protection and privacy law when sharing Data

3.2.1 Data Sharer represents that:

(i) the collection and sharing with the Data Recipient of Data which qualifies as personal data within the meaning of Article 4 (1) of Regulation (EU) 2016/679 ("Personal Data")

complies with this regulation ("GDPR") as well as any other applicable data protection law; and

(ii) where relevant, that the requirements of Article 5 (3) and generally the applicable provisions of Directive 2002/58/EC were complied with upon collection of Data.

3.2.2 Each Party represents that it will process Personal Data in relation to data processing activities contemplated by this Contract in accordance with GDPR,, Directive 2002/58/EC and national implementing legislation as well as any other applicable data protection law.

3.2.3 Appendix 3 contains 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 allows to link the data to identified or identifiable individual. This can happen also 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 the 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 Data Sharer is controller or 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 Recipient using data for its 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 Art 26 GDPR. They must jointly arrange how they comply with the GDPR.
- Where the GDPR imposes specific terms to apply (e.g. under Article 26 or Article 46), such terms can (and should) be merged with these Model Contractual Terms, for example by being included in **Appendix 3**. **Appendix 3** should generally specify how the requirements set out in the GDPR are fulfilled, including with regards to the respective role and responsibilities of the Parties under GDPR.

**Valid legal basis**

A valid legal basis under Art 6(1) GDPR to share the data should exist and the data subject has to be informed about that (further) processing according to 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 the consent, contract or legitimate interest.
- Data can only be shared for specified, explicit and legitimate purpose. 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.
- Data Sharer acting as a controller could also share - on the basis of its legitimate interest to better retain clients in the future - the data with its mother company acting also as an independent data controller and using the data to create global statistics – on the basis of its legitimate interest to improve the services globally provided by the group.

Data recipients should receive sufficient information from Data Sharer to be able to demonstrate its 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 are initially collected under article 6(4) GDPR in case of joint controllership. All the necessary details about the respective obligations of the parties, legal basis, information and rights of data subjects 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 EU/EEA:

  https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en

### 3.3 Incorrectness of fundamental representations and warranties

3.3.1 Any Party that becomes aware that any representation or warranty referred to in this clause is not, or no longer, correct, or will no longer remain to be correct 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. Where a Party is aware of the incorrectness of fundamental representations

or warranties and fails to notify the other Party, it shall be liable in line with applicable law to the other Party for direct damage suffered as a result, including as a result of reliance on this Contract.

3.3.2 On becoming aware of this situation, each of the Parties must take appropriate action and cure the false or incorrect fundamental declaration, to the extent possible. If the situation is not and cannot be cured, this Contract must terminate by means of a written termination notice mentioning the reasons of termination given by either party to the other. The termination has immediate effect. Where the incorrectness 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 9.4. This does not remove: data subjects' rights under data protection law; any obligations, rights or remedies following from other EU law or applicable national law, such as provisions on mistake, fraud, duress or undue influence; any liability of either Party towards any protected third party.

## 4. Making the data available

### 4.1 Data quality

> Data Sharer can take various degrees of commitment regarding the data provided, from the most basic commitment that it will be provided with the metadata making it intelligible – a bare consequence of good faith in the conclusion of the Contract – to the most stringent commitment that it will fit the purposes contemplated by the Recipient and/or be exhaustive and accurate. The Parties could select as many options as they please 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 is 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 in conformity with the conditions set out below:

Basic commitment: The Data Sharer shall make the data available to the Data Recipient:

(a) in the same quality as it's available to the Data Sharer; and

(b) together with the relevant metadata, domain tables, semantics, licensing information and other information required for intelligibility of the Data by the Data Recipient.

[OPTION] and *[Please select, if applicable, one or more options as appropriate]*

☐ Data is made available in a comprehensive, structured, commonly used and machine-readable format. The Parties consider this requirement as fulfilled by the following specifications concerning the Data: *[Please describe as applicable]*

☐ The Data Sharer shall make the data available to the Data Recipient in accordance with the FAIR (Findable, Accessible, Interoperable, Reusable) principles as further described in https://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 to assess 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 is available and meets 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 Sharer represents that the Data is adapted to the following context of processing by the Data Sharer in accordance with usual expectations: [*Please add a brief description]*

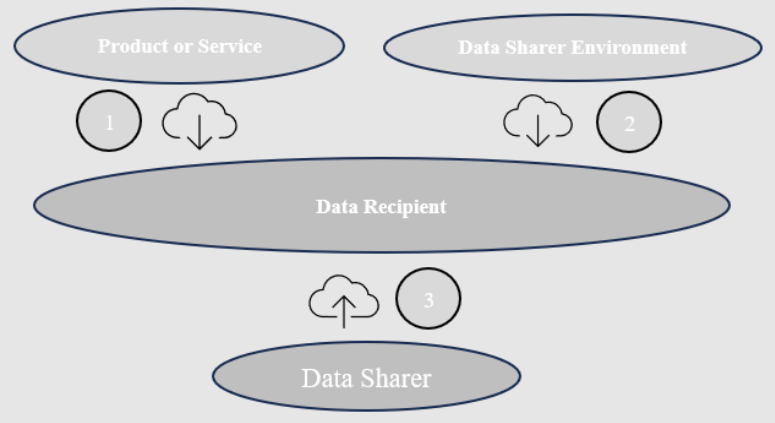
☐ The Data Sharer represents that the Data is fit for the objectives pursued by the Data Recipient: [*Please add a brief description]*

☐ Specific quality requirements: The Data Sharer shall make the following available to the Data Recipient: [*Please add/remove/complete specific quality requirements]*

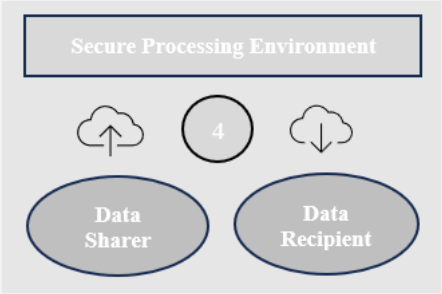
- An exhaustive dataset, meaning that Data contains all the data in possession of the Data Sharer related with the scope of this Contract; and/or
- An up-to-date dataset, meaning the Data reflects the data in possession of the Data Sharer at the date of signature of this Contract; and/or
- An accurate dataset, meaning the Data has been curated by the Data Sharer and is – to the best of its knowledge – error free, correct and reliable; and/or
- A dataset which is compliant with the following standards: [X] (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: [X]

## 4.2 Obligations of the Data Sharer in relation to the access to Data

The Data Sharer may make the Data available in different ways, either giving or retaining technical control of the Data (without prejudice of 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 (scenario 1) or from the environment of the Data Sharer (scenario 2), or that the Data Sharer oversees the transferring of Data to the Data Recipient (scenario 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 a secure processing environment - as defined under Article 2, point (20) of Regulation (EU) 2022/868 – especially in a situation where personal data is concerned (scenario 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. Beside legal safeguards regarding personal data that are described in 3.2. (respectively in **Appendix 3**), security measures (as further described in **Appendix 4**) should cover technical and organizational aspects as well regarding e.g.:

- Data confidentiality by access control and secure data flow
- Data retention & deletion provisions
- Data integrity- and monitoring measures
- Data breach provisions

4.2.1 Access modalities. The Data Sharer shall make the Data available to the Data Recipient by:

*(Please select all options that apply)*

☐ **[1st OPTION: Retrieval by the Data Recipient from Products or Services]** Enabling retrieval directly from the following products and/or services not hosted by the Data Sharer, including by making any required technical specifications available (e.g. communication protocol) to allow the Data Recipient to retrieve the Data ("**Specifications**"): *(Insert method and products/services not hosted by the Data Sharer)*

☐ **[2nd OPTION: Retrieval by the Data Recipient from the environment of the Data Sharer**] Enabling retrieval in the Data Sharer´s environment, including by making any required Specifications of the Data available, 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]*

Where Specifications are provided to the Data Recipient under OPTION 1 or 2, the Data Sharer hereby authorizes 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 it shall have no other right, interest or license in or to the Specifications.

☐ [**3rd OPTION: 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[*

☐ [**4th OPTION: Access by Data Recipient to the environment of 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 with the non-transferable, non-sublicensable right to access its environment available as above mentioned only for the purpose and the duration specified in this Contract; Data Sharer reserves the right to suspend access to its environment if incompliant use is detected.

In each of the above-mentioned OPTIONS 1 to 4, the environment of the Data Sharer and the environment of the Data Recipient shall be deemed to include:

- Environment of any third-party designated by the concerned party to hold or receive the Data on its behalf (including as appropriate any secure processing environment as defined under Article 2(20) of Regulation (EU) 2022/868),
- 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 is accessed by the Data Recipient in a privacy-preserving manner.
>
> In the case of Federated Learning, the data is "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.

4.2.2 Timing, updates, retention period.

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 make such updated or corrected version available to the Data Recipient without undue delay after it becomes available to the Data Sharer. Where the Data is continuously updated and corrected, it will be made available to the Data Recipient *[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 *[to be specified]* thereafter.

[OPTION] The Data is retained by the Data Sharer for a duration of *[Insert retention period as applicable for Data Sharer*], after which it will not be available anymore for the Recipient to access.

4.2.3 Provision of necessary means and information. The Data Sharer must provide Data Recipient with the means and information strictly necessary for accessing or receiving the Data in accordance with this Contract. This includes, in particular:

(a) [OPTION where the data is not provided in a standard format] the provision of software and an accompanying license 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 requirements includes the following: *[Insert further details.]*

**4.3 Obligations of the Data Recipient in relation to the access to Data**

4.3.1 Retrieval or access to the Data. 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 case of access to the Data in the Data Sharer's environment) The Data Recipient warrants that:

(a) only employees who work for or with the Data Recipient and whose duties strictly necessitate such 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) The Data Recipient will not: (a) authorize or facilitate any third party to access the Data Sharer's environment; or (b) 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 of the Data Sharer's environment; or (c) 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 optimization for integration], or circumvent or bypass any security mechanism of the Data Sharer's environment; (d) 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 represents that it will ensure the confidentiality, integrity and availability of the data by defining appropriate security measures in Appendix 4 when making the data available under one or more options under 4.2.1.

4.4.2. Changes in the data to be shared or its environment may affect the agreed security measures. Data sharer and data recipient agree to evaluate the security measures [*regularly / upon request of the other party/ upon special events (to be specified)*, and to agree in good faith upon any necessary adaptation.

4.4.3 Each party shall provide the other party upon request with a detailed documentation of the security measures implemented in accordance with this article and Appendix 4 of this Contract.

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) the 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 Duty to renegotiate. Should any of the specifications concerning data quality, access modalities or necessary means and information to access and use of the Data appear – at any time following the signature of this Contract - to be insufficient to fulfil the objectives pursued by one or both of the Parties, the Parties undertake to enter into negotiations and adapt the specifications so that they meet said objectives.

4.5.2 Non-compliance of the Data. 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 quality 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 of the incident. If the incident was caused by failure of the Data Sharer to comply with their obligations, they must remedy the breach [within a reasonable period of time] OR [within a time period of (…)]. If the Data Sharer does not do so, it is considered as a fundamental

breach and the Data Recipient may invoke clause 10 of this Contract (remedies for breach of contract).

4.5.3 Impossibility to meet the agreed specifications. If any of the specifications agreed in accordance with clauses 4.1 to 4.2 are impossible or unreasonable to achieve because of a change of circumstances, the Data Sharer must notify the Data Recipient with a detailed description of this and the Parties will enter into negotiations in good faith and adapt the specifications. In particular, each Party must provide to 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 clauses 10.

4.5.4 Unilateral changes. The Data Sharer may, in good faith, unilaterally change details regarding the specifications for the data and access arrangements, if this is objectively justified by the conduct of business of the Data Sharer – for example by a change in the Data Sharer's infrastructure. In any case, the specifications must meet the requirements of clauses 4.1 and 4.2.

The Data Sharer must in this case give notice of the change to the Data Recipient without undue delay after deciding on, or learning about, the change. Where the change may affect data access and use by the Data Recipient more than just to a small extent, the Data Sharer must give notice to the Data Recipient at least (indicate a reasonable period of time) before the change takes effect.

A shorter notice period may suffice where such notice would be impossible or unreasonable in the circumstances, such as where immediate changes are required because of a security gap that has just been detected.

Where the change has detrimental impact on the Data Recipient, then the Parties undertake to work jointly together to mitigate such impact, and absent satisfactory mitigation measures the Data Recipient may terminate without any compensation being due to the Data Sharer.

## 5. Use of the Data and disclosure to third parties

### 5.1 Use of Data

5.1.1 Authorized use [Please select only one option]

[RESTRICTIVE OPTION] The Data Recipient may process the Data only for the purposes of: *[Insert authorized purposes]* ("Authorized Purposes").

OR

[BROAD OPTION] The Data Recipient may process the Data for any purpose ("Authorized Purposes") [OPTION] (*if applicable*) other than the prohibited practices exhaustively listed below *(examples only)*

- use the data it receives for any purposes that are in violation of Union law or applicable national law;

- *(If applicable)* if the data is Product data, use the data it receives to develop a product that competes with the Product;
- 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)* if the data is Product Data or Related Services Data obtained under Article 4 or 5 or the Data Act, share the data directly or indirectly with a third-party considered as a gatekeeper under Article 3 of Regulation (EU) 2022/1925;
- Other: *[specify*]

5.1.2 Authorized operations on the Data (Please select only one option)

[RESTRICTIVE OPTION] The Data Recipient may only implement the following operations on the Data: *[Insert authorized operations e.g., access and copy Data to create aggregated statistics in relation to the Authorized purposes]* ("Authorized Operations").

OR

[BROAD OPTION] The Data recipient may implement on the Data any operation ("Authorized operations") other than the prohibited operations exhaustively listed below *(examples only)*:

- *(If applicable)* if the data is Product data, use the data it receives in a manner that adversely impacts the security of the Product or any Related Service;
- [OPTION] Host or otherwise transfer or make accessible data outside of the European Union;
- Intent to re-identify data subjects where the Data has been previously anonymized or pseudonymized by the Data Sharer;
- Other: *[specify*]

5.1.3 Furthermore, the Data Recipient undertakes not to engage in the following conduct for the purposes of obtaining data or any other purpose:

- provide false information to the Data Sharer;
- deploy deceptive or coercive means;
- 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 [in perpetuity / for the duration of the Contract / for a duration of (*please 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 its right to use the Data, the Data Recipient undertakes to permanently delete the Data (including any copy or backup) and to ensure any third parties to whom the Data has 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 Disclosure of data to third parties

5.2.1 The Data Recipient shall not share or transfer any Data to any third party, whether in identified, anonymized or pseudonymized or aggregate form, except that the Data Recipient may share Data solely as follows: [fill as appropriate]

5.2.2 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) impose the same or substantially equivalent obligations on the third party that arise for the Data recipient from this contract. This includes in particular but without limitation the Data Recipient's obligations to:

- make sure – especially by means of contractual arrangements – that the third party applies at least the same security measures and obligations agreed by the Data Recipient under clause "Security measures", and
- make sure that the third party uses the data exclusively in a way compatible with clause "Use of the Data"; and
- [OPTION] take appropriate technical and organisational measures to 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.
- impose upon the third party to ensure that all subsequent third parties receiving the Data comply with the obligations set out in this contract.

[OPTION] This article should not apply if the third party is a Data intermediation service under the DGA or any other service provider and does not process the Data for its own business purpose.

## 6. (if the data is protected as trade secrets) Trade Secrets

**About Trade Secrets:**

Trade Secrets are confidential information that confers a competitive advantage to a company. According to Article 2 (1) of the Trade Secrets Directive, to be eligible for trade secret protection, information needs to meet three requirements:

- It must be secret,
- It must have a commercial value because of its secrecy,
- Information-Holder must take reasonable steps to keep it 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 means to keep data secret and therefore trade secret protection could take place.

**How to deal with trade secrets?**

If Data Sharer identifies that certain trade secrets are 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 condition to sharing those identified trade secrets, such as taking certain additional technical and organisational measures in order to preserve the confidentiality. Data Sharer and Data Recipient should, in **Appendix 2** as part of the Contract, include all the details on the Data which are protected as trade secret.

### 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 shared by the Data Sharer to the Data Recipient, which are protected as trade secrets within the meaning of the Trade Secrets Directive, held by the Data Sharer or another Trade Secret Holder within the meaning of the same Directive, and which was brought to the attention of the Data Recipient in a clear and comprehensible manner, in writing, before the conclusion of the Contract (hereafter 'Identified Trade Secrets').

6.1.2 The Identified Trade Secrets and the identity of the Trade Secret Holder(s) are set out in the Appendix 2. Either the Data Sharer or, if different, the Trade Secret Holder, shall be responsible for identifying Identified Trade Secrets prior to the conclusion of the Contract and where relevant, during the course of the Contract, and shall inform the Data Recipient of such Data accordingly.

6.1.3 The obligations set forth in this article remain in effect after any termination of the Contract, unless otherwise agreed by the Parties or unless the Data Recipient is able to demonstrate that the Identified Trade Secrets have become generally known among or readily accessible to

persons within the circles that normally deal with the kind of information in question, for causes different from its unauthorized disclosure by the Data Recipient.

### 6.2 Protective measures to be taken by the Data Recipient

The Data Recipient shall apply the protective measures as set forth in the Trade Secrets section of **Appendix 2** (hereinafter: 'Identified Trade Secrets DR Measures').

> Parties should include in **Appendix 2** 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 (e.g. internal governance, appropriate identity management and access controls, involvement of a trusted third party) nature.
>
> The measures will depend on whether access is to be provided in situ or on whether the data is to be fully transferred to the Data Recipient, as in the former case the Data Sharer or trusted third party has a higher degree of control and can apply part of the protective measures itself.

### 6.3 Protective measures taken by the Data Sharer

The Data Sharer may apply appropriate technical and organisational protection measures if and to the extent set out in detail in the Trade Secrets section of **Appendix 4** to preserve the confidentiality of the shared and otherwise disclosed Identified Trade Secrets (hereinafter 'Identified Trade Secrets Data Sharer Measures'), while ensuring compliance with Union law or applicable national law as well as with the data sharing and other contractual obligations of this Contract.

The Data Recipient undertakes not to alter or remove such Identified Trade Secrets Data Sharer Measures unless otherwise agreed upon by the Parties.

### 6.4 Third party Identified Trade Secrets Holders

6.4.1 The Data Sharer herewith represents to the Data Recipient that it has any and all relevant authorisations and other rights of (each of) such third party Identified Trade Secrets Holders to enter into this Contract regarding the applicable Identified Trade Secrets and any and all of the related rights and obligations hereunder.

6.4.2 Identified Trade Secrets Data Recipient Measures and Identified Trade Secrets Data Sharer Measures reflect the contractual commitments of the Data Sharer towards the initial Data Holder. Should such commitments from Data sharer towards the initial Data Holder evolve, in such case the Data Recipient commits to align on any new measures agreed upon between the Data Sharer and the initial Data Holder.

6.4.3 (if applicable because data was initially obtained by the Data Sharer under mandatory data sharing) Should the initial Data Holder suspend or terminate sharing of Data or Identified Trade Secrets in accordance with the Data Act, the sharing of such Data or Identified Trade Secrets

between the Data Sharer and the Data Recipient will automatically and accordingly be suspended or terminated upon notification by the Data Sharer.

## 7. Intellectual Property Rights

"Intellectual Property Rights" means copyrights (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, knowhow and confidential and undisclosed information (such as inventions, whether patentable or not), rights in logos and patents, sui generis rights in database and any other rights recognized under applicable law.

The data in 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 it is the person who made the substantial investments in terms of quality or quantity for the acquisition, verification or presentation of its content. The maker can prohibit extraction and reutilization 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 harmonized and may therefore vary between Member States.

**Patents:**

Data sharing and use of the data can lead to inventions as they inspire new ideas, optimize 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 of the contract 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 (if the Data is covered by intellectual property rights) Subject to the payment of the compensation under this Contract, the Data Sharer hereby grants the Data Recipient for the term of the Contract, worldwide, non-exclusive, non-transferable license, to use, copy, modify, enhance and maintain the Data that would be covered by an Intellectual Property Right solely to the extent necessary under the Contract. A sublicense to Recipient's subcontractors is authorized 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 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 its 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 agreement 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 The Parties moreover agree that further licensing on the Results shall be granted as follows: [select as many options as appropriate]

[OPTION 1] [*Party which does not own IPR on the results*] hereby grants to 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 license 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] [*owner of the IPR on the Results*] hereby grants to 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 license to use, copy, modify, enhance and maintain the Results solely for the following purposes: [*please fill as applicable*]

## 8. Compensation for provision of data access

> Parties may, in the Contract itself or in a separate Appendix, determine details on compensation 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 license fees as the case may be. Parties should agree, at least, on the following: amount of compensation due, and the relevant currency; time when payment is due; and modalities of payment.
>
> They may agree on further compensation, where applicable, for additional services which shall be subject to an additional fee.

The Parties agree that the Data Recipient will compensate the Data Sharer as follows: *[fill as appropriate]*

## 9. Date of application, duration of the Contract and termination for convenience

### 9.1 Date of application

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]*.

> Parties should agree, at least, on the following: amount of compensation due, and the relevant currency; time when payment is due; and modalities of payment.

### 9.2 (if applicable) Duration

This Contract [OPTION 1] is made for the period of *[insert period*], [OPTION 2] comes into effect on *[insert date]* and is concluded for an indeterminate period, subject to any grounds for termination under this Contract.

> 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. 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 9.2, depending on whether the Requesting User has specified a particular time period.

### 9.3 Termination for convenience

9.3.1 The Data Recipient may terminate the Contract at any time before the start of [(if applicable) or during] the contract period by giving the Data Sharer a notice of [*insert period*].

9.3.2 [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: *[please specify]*

> There may be cases where the Data Sharer 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 Sharer may want to make sure that they receive compensation from the Data Recipient.

### 9.4 Effects of expiry or termination

9.4.1 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 11.7 or any other provision which is to operate even after the contract has come to an end.

9.4.2 The Parties must take appropriate and reasonable steps to prepare for expiry of the contract period or termination of this Contract. [OPTION 1] This may, depending on the circumstances, include such exit support measures as the Data Recipient may reasonably expect. [OPTION 2] This includes the following exit support measures:

> 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.

9.4.3 On termination of this Contract a Party may recover money paid for a performance which they did not receive or which they properly rejected. A Party that has rendered performance which can be returned and for which they have not received payment or other counter-performance may recover the performance. A Party that has rendered a performance which cannot be returned and for which they have not received payment or other counter-

performance may recover a reasonable amount for the value of the performance to the other Party.

## 10. Remedies for breach of Contract

### 10.1 Rights and remedies

The rights and remedies provided under this Contract in case of breach are in addition to, and not exclusive of, any rights or remedies provided by law. Remedies which are not incompatible may be cumulated. In particular, the aggrieved Party is entitled to claim damages in addition to the exercise of any other remedy.

### 10.2 Non-performance

10.2.1 A non-performance of an obligation amounts to a fundamental breach to this Contract if:

(a) strict compliance with the obligation is of the essence of this **Contract**, in particular because non-compliance would cause significant harm to the other Party, or other protected third parties; or

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

(c) the non-performance is intentional and gives the aggrieved Party reason to believe that it cannot rely on the other Party's future performance

10.2.2 A Party’s non-performance is excused if it proves that it is due to an impediment beyond its control and that it 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 within a reasonable time after the non-performing Party knew or ought to have known of these circumstances. The other Party is entitled to damages for any loss resulting from the non-receipt of such notice

### 10.3 Remedies for breach

In the event that any Party fails to comply with its obligations under this Contract, the other Party shall have the following remedies:

(a) Right to Terminate: Each Party shall have the right to immediately terminate this Contract, without penalty, if

(i) the other Party's non-performance is a fundamental breach,

(ii) if the other Party breaches any material obligation and fails to remedy such breach within [30] days of receiving written notice of such breach

(b) Damages for breach: The aggrieved Party is entitled to damages for any pecuniary loss, damage, or injury suffered due to a breach of the Contract which is not excused under clause 10.2.2, including but not limited to a breach concerning use or provision of the data, loss of personal data, unauthorized access, or misuse of data, caused by the other Party's non-performance.

The non-performing Party is liable only for loss which it foresaw or could reasonably 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.

The amount of damages shall be based on the actual loss suffered by the aggrieved Party, including any consequential and incidental damages, to the extent permitted by law. [This amount shall not exceed [specify] EUR.]

(c) Specific Performance: In the case where a Party fails to perform its obligations other than a monetary performance, the aggrieved Party may request that the non-performing Party comply, without undue delay, with its obligations under this Contract. The aggrieved Party may apply to court for an order for specific performance of the Contract if permitted by applicable law.

Specific performance cannot, however, be obtained where:

(i) performance would be unlawful or impossible; or

(ii) performance would cause the other Party unreasonable effort or expense; or

(iii) the performance consists in the provision of services or work of a personal character or depends upon a personal relationship, or

(iv) the aggrieved Party may reasonably obtain performance from another source

### 10.4 Agreed Payment for Non-performance

[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 10.3 (b). 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 loss resulting from the non-performance and the other circumstances.]

## 11. General provisions

**11.1 Confidentiality**

11.1.1 The following information must be considered confidential:

- 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;

- information setting out the basis for the calculation of the reasonable compensation;

- information referring to the Requesting User and any other protected third party, unless the protected third party has made this information public;

- [OPTION] the existence of this Contract and the identity of the Parties;

- [OPTION] the terms and conditions of this Contract;

- information referring to the performance of this Contract and any disputes or other irregularities arising in the course of its performance.

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 one of the Parties:

(a) is under a legal obligation to disclose or 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) has to disclose or make available the relevant information to meet its obligations under this Contract, and the other Party (or the party providing the confidential information or affected by its disclosure) can reasonably be considered to have accepted this; or

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

11.1.3 In any case, the Data Sharer 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 Sharer to demonstrate compliance with its obligations (i) in respect of the Data Recipient

requesting third party 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.

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

11.1.5 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 EU or Member State law.

**11.2 Non-discrimination**

The Data Sharer declares that – with the terms of this Contract and any practices related to its fulfilment – when making data available, they 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.

If the Data Recipient considers the conditions under which data has been made available to them to be discriminatory, the Data Sharer must, on request by the Data Recipient, demonstrate that there has been no discrimination.

**11.3 Applicable law**

This Contract is governed by the law of [specify state].

**11.4 Entire Contract, modifications and severability**

11.4.1 This Contract (together with its appendices and any other documents referred to in the a 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.

11.4.2 Any modification of this Contract will be valid only if agreed to by the Parties in writing, including in any electronic form that is considered to meet the requirements of a written document (in line with good commercial practices).

11.4.3 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 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 according to clause 11.5.

**11.5 Interpretation**

11.5.1 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 EU law or national legislation adopted in accordance with

EU law, as well as any applicable national law that is compatible with EU 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 11.3) and, in any case, according to the principle of good faith and fair dealing.

### 11.6 Notifications

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:

(d) if delivered by hand, on the date of delivery;
(e) if sent by prepaid post, on the third business day after posting;
(f) 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.

### 11.7 Dispute settlement

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 competences 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*].

**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 (SCCs)

### (a) Purpose of the standard contractual clauses

Article 41 of the Data Act requires the Commission to develop and recommend non-binding standard contractual clauses for cloud computing and other data processing services contracts ('SCCs') to assist parties to draft and negotiate contracts with fair, reasonable and non-discriminatory rights and obligations.

The SCCs, proposed by the Expert Group are intended as best practice guidance to assist the contractual implementation of the rights and obligations stemming from the Data Act and their use is fully voluntary. They are a set of modular clauses which largely complement each other but can also be used separately. The parties to a contract can complement and adapt these SCCs to their individual contractual needs, including with regard to specific EU and Member States' law, where such specific law applies. The clauses are meant to be inserted by the parties into their data processing services agreements.

### (b) For whom?

The SCCs aim to help any Customer or Provider. This includes any Customer of any data processing service, whether public, private or otherwise, small, midsized or large.

The SCCs aim to assist in particular companies that may not have sufficient experience or resources needed to draft and negotiate contracts with fair, reasonable and non-discriminatory contractual terms.

A. **SCCs General** with **Annex Definitions** *[link]*;
B. **SCCs Switching & Exit** *[link]*, with **Annex Switching & Exit Plan** *[link]*;
C. **SCCs Termination** *[link];*
D. **SCCs Security & Business Continuity** *[link]*;
E. **SCCs Non-Dispersion** *[link]*;
F. **SCCs Liability** *[link]*, and;
G. **SCCs Non-Amendment** *[link]*.

Below, there is a brief overview of the specific SCCs. Detailed explanations are included in the respective SCCs both in their introduction and as *Info Points*, listed at the end of each set of 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.

In line with the definition of a data processing service in the Data Act, these SCCs are applicable to all cloud service models, including IaaS, PaaS, and SaaS.

### (c) What do the SCCs consist of?

**SCCs General**

The SCCs General provide for a generic structure and elements, which are common to other, topic-specific SCCs. It also includes other relevant topics that generally need to be part of an agreement for data processing services. Furthermore, these SCCs comprise of the main definitions used across the other SCCs.

**SCCs Switching & Exit**, with **Annex Exit Plan**

The Data Act ensures that any obstacles to switching are removed: technical, pre-commercial, commercial, contractual, organisational ones.

These SCCs translates the new rights and obligations introduced by the Data Act as regards the switching and exit process into contractual terms. The SCCs set out the switching process when moving from one Provider to another as well as from the cloud to on-premise infrastructure. They cover the process and timelines for switching, responsibilities of the parties involved, assistance to be made available to the Customer (and any third parties authorised by the Customer), and further related topics mandatory under the Data Act.

**SCCs Termination**

These SCCs cover the service contract termination process. They are directly linked to the SCCs Switching & Exit and provide for the various termination possibilities and related conditions. The data processing agreement is usually terminated (in full or partially) once the switching process has been concluded successfully or if the Customer does not wish to switch to another Provider but requires 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.

**SCCs Security & Business Continuity**

These SCCs are based on the requirement of the Data Act 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.

While the topics of security and business continuity is generally already included in the data processing agreement and other contractual documentations, however, these SCCs focus on the importance of security and business continuity with relation to the switching and exit process as per the rights and obligations introduced by the Data Act.

**SCCs Non-Dispersion**

The SCCs Non-Dispersion provide for information and communication symmetry. Data processing agreements often comprise of various ancillary documents, which refer to additional material and information, which can be widely dispersed across different repositories. This makes it difficult for prospective Customers to find all the information they need to assess the parties' contractual and legal obligations and their implications. These SCCs are, therefore, intended to help easy and practical access to relevant updated information, documents, materials and contact details by both Customer and Provider.

**SCCs Liability**

These SCCs Liability assist the parties in defining balanced and mutually appropriate liability terms. In particular, small and mid-size companies and other organisations may find these SCCs helpful when they negotiate and/or draft liability provisions in their Agreements. The clauses also point at some issues that organisations, irrespective of their size, may not have thought of.

While the Expert Group acknowledges that a clause on liability is usually included in the general Agreement between the Customer and the Provider, the experts believe it is useful to include optional provisions on liability in the SCCs as they reflect the spirit of the Data Act of the importance of fair, reasonable and non-discriminatory rights and obligations, including those related to the cloud computing contracts and the switching process.

**SCCs Non-Amendment**

It is important that the parties can rely on the rights and obligations they agreed to contractually and that these rights and obligations are not changed or otherwise amended unilaterally, unless under clearly and mutually agreed conditions.

The SCCs Non-Amendment are intended to give more clarity and confidence to the parties when agreeing on terms pertaining to unilateral changes. The SCCs address possible contractual arrangements to help ensure that unilateral changes are not detrimental to the interests of either party.

### (d) How to use the SCCs?

It is recommended to start with and from the SCCs General, in which the complete set of SCCs is mentioned. The complete set of SCCs was developed to be consistent with and mutually reinforcing each other. Although not necessary, it is recommended to use the entire set of SCCs.

Each of the SCCs first explains the chosen approach or specific situations covered. It is recommended to familiarise oneself with these explanations.

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

The parties can discuss, negotiate, and agree to cover a multitude of services in one, single agreement, which may be called master services agreement or otherwise ('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 may decide to switch one or a given number of services to a new, designated Provider, the Agreement will continue to be in force for the other services.

Please note that, if other definitions 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.

If you intend to use these SCCs only partially or to make changes to them, you should carefully consider how this might affect the contractual rights and obligations.

**Legal and other professional advice is always recommended in such situations!**

In any case, the s the users of these SCCs, whether Customers, Providers or others, decide how to use the SCCs, entirely or partially, or not to use them .

**Please also note these General Information Points**

There may be additional rules and requirements applicable to cloud computing in specific sectors which should also be considered (for example, in the financial, health, telecom, industry, energy or public sector, to name a few).

Throughout the relation and legal lifecycle between Customer and Provider, keep in mind the obligation of good faith on the parties, as mentioned explicitly in Article 27 of the Data Act.

Please also note that the Data Act provides for exceptions to certain obligations related to the SCCs Switching & Exit. Reference is made to Article 31 Data Act. Further explanations can also be found in the SCCs Switching & Exit.

**Standard Contractual Clauses (SCCs)**
**For Data Processing Services**
including without limitation: cloud computing services

**SCCs General**

## A. Explanatory notes for users of the SCCs General

SCCs General provide for a generic structure and components to cater for, include, combine or otherwise refer to the specific SCCs. It also includes other relevant topics that generally need to be part of an agreement for cloud computing and other data processing services.

These SCCs General also comprise of the main definitions of each of the SCCs, which can be found in the Annex Definitions, which is an integral part of these SCCs General.

The SCCs General assist both Customer and Provider (collectively: 'Parties') to create and validate a complete, coherent set of SCCs that are fair, reasonable and non-discriminatory.

Please note there may be additional requirements applicable to cloud computing in specific sectors which should also be considered (for example, in the financial, health, telecom, industry, energy or public sector, to name a few). Also for that reason, it is recommended that the Customer identifies, establishes and indicates in the Agreement if and to what extent they are a customer that is subject to the NIS2 Directive (EU) 2022/2555 (NIS2), Critical Entities Resilience Directive (EU) 2022/2557 (CER), and/or the Digital Operational Resilience Act (EU) 2022/2554 (DORA).

Please keep in mind the obligation of good faith on the parties (including the destination providers of data processing service providers) throughout the relation and legal life cycle between Customer and Provider, both before entering into an Agreement, during as well as after. This is explicitly mentioned in Article 27 Data Act.

Please also note that the Data Act provides for certain exceptions to certain obligations related to the SCCs Switching & Exit. Reference is made to Article 31 Data Act. Further explanations can be found in the SCCs Switching & Exit.

**SCCs General**

**Agreement**

1. Customer and Provider agree that Provider will make available to Customer certain Services on and in accordance with the terms of this Agreement, which – amongst other – consists of the following documents (hereinafter collectively referred to as the '*Agreement*'):

    A. SCCs General, with Annex Definitions *[link]*;
    B. SCCs Switching & Exit *[link]*, with Annex Switching & Exit Plan *[link]*;
    C. SCCs Termination *[link]*;
    D. SCCs Security & Business Continuity *[link]*;
    E. SCCs Non-Dispersion *[link]*;
    F. SCCs Liability *[link]*;
    G. SCCs Non-Amendment *[link]*.

2. The aforementioned SCCs separately and collectively form an integral part of the Agreement. Any reference to the Agreement shall be deemed to include a reference to said documents.
3. The agreement between Parties on the above supersedes and replaces any previous arrangement, understanding or agreement, whether written or oral, between the Parties with respect to the subject matter in the aforementioned documents. Changes or other amendments or supplements to the Agreement are only valid and effective if these are agreed upon in writing between Parties, except as otherwise expressly set forth in the SCC Non-Amendment.

**Definitions**

4. The definitions used and applicable in these SCCs General, the other SCCs as well as the other documents that are part of the Agreement are set forth in the Annex Definitions, hereunder.

**Order of precedence**

5. In the event of any conflict or inconsistency between these SCCs General and the other SCCs on the one hand, and on the other hand any other applicable contractual arrangements, terms, conditions or other (parts of) applicable agreements related to the topics of these SCCs– including any policies, information, documentation, schedules, exhibits, annexes or the like pertaining to them –, these SCCs General and the other SCCs will take precedence with regard to the topics related to them.

**Miscellaneous**

6. This Agreement is governed by the national laws of *[ insert name of Member State]*.
7. In case of any conflict or other dispute between Parties under or related to this Agreement, Parties will discuss and aim to amicably settle the matter at hand in good faith in line with Article 27 Data Act but without prejudice to any rights and remedies each Party may have.
8. On the latter, Parties can resort to the remedies by applicable law or under the Agreement and – if needed – refer the dispute to the competent court in *[insert competent court in a Member State.]*

**Info points - General**

*The Data Act itself also caters for additional possibilities, being (A) Customer and the Provider*

*have access to a dispute settlement body designated by Member States in accordance with Article 10.4 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) Data Act.*

*However, please do note that the Member States define the tasks and powers of the competent authority designated by the relevant Member State, and these may vary to a certain extent. It is therefore possible that such authority is not competent to settle disputes between the Customer and the Provider. The Parties must, therefore, assess the most appropriate way to oblige the other party to fulfil its legal and contractual obligations, and how to settle disputes.*

**Annex**
**Definitions**

The following definitions in these SCCs General, the other SCCs as well as the other parts of the Agreement (including its Annexes) as agreed between Parties, will have the following meaning:

1. **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 performance of the Agreement(s), including without limitation its Annexes;

2. **Annex** means an annex, schedule or exhibit explicitly referenced in the Agreement;

3. **Customer** as defined in Article 2(30) Data Act: 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.

   For purposes of this Agreement, said Customer is the legal entity, person or organisation with whom Provider wishes to enter into, enters into or has entered into a legal relationship regarding providing Services by Provider, as well as related matters. There is no sectorial limitation under the Data Act, whether a Customer is part of the private, public, public-private or any other sector;

4. **Data** as defined in Article 2(1) Data Act. For easy reference: 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;

5. **Data Act** means Regulation (EU) 2023/2854 (‘DA’);

6. **Data egress charges** as defined in Article 2(35) Data Act. For easy reference: data transfer fees charged to Customers for extracting their data through the network from the ICT infrastructure of the Provider of Data Processing Services to the system of a different provider or to on-premises ICT infrastructure;

7. **Data Processing Service** as defined in Article 2(8) Data Act. For easy reference: 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 Provider to Customer as agreed under the Agreement, not being Other Services;

8. **Destination Provider** as mentioned in Article 2(34) Data Act, means the destination provider of data processing services, whereby the Customer changes from using the Data Processing Services from Provider to using another data processing service of the same service type, or other service, offered by such different provider of data processing services, or to an on-premises ICT infrastructure, including through extracting, transforming and uploading the data;
9. **Digital assets** defined in Article 2(32) Data Act. For easy reference: 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;

10. **Exportable data** as defined in Article 2(38) Data Act. For easy reference: 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 the Provider or third parties;

11. **Functional Equivalence** as defined in Article 2(37) Data Act. For easy reference: re-establishing on the basis of the customer's exportable data and digital assets, a minimum level of functionality in the environment of a new data processing service of the same service type after the switching process, where the destination data processing service delivers a materially comparable outcome in response to the same input for shared features supplied to the Customer under the Agreement;

12. **Interoperability** as defined in Article 2(40) Data Act. For easy reference: 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;

13. **Maximum Notice Period** as defined in Article 25(2)(d) Data Act, and within that meaning further defined in the SCC Switching and Exit, as agreed between Parties under the Agreement;

14. **Mandatory Maximum Transitional Period** md as defined in Article 25(2)(a) Data Act, and within that meaning further defined in the SCC Switching and Exit, as agreed between Parties under the Agreement;

15. **Metadata** as defined in Article 2(2) Data Act . For easy reference: a structured description of the contents or the use of data facilitating the discovery or use of that data;

16. **Minimum Period of Data Retrieval** as defined in Article 25(2)(g) Data Act, and within that meaning further defined in the SCC Switching and Exit, as agreed between Parties under the Agreement;

17. **Non-personal Data** as defined in Article 2(4) Data Act. For easy reference: data other than Personal Data;

18. **On-premises ICT infrastructure** as defined in Article 2(33) Data Act. For easy reference): 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;

19. **Other Services** means all professional services of whatever nature to be provided by Provider to Customer under the Agreement as defined therein, that are not Data Processing Services;

20. **Party** or **Parties** means Customer or Provider, respectively Customer and Provider;

21. **Personal Data** as defined in Article 4, point (1), of Regulation (EU) 2016/679 (General Data Protection Regulation ('GDPR'));

22. **Plan** means the switching and exit plan referred to in the SCC Switching and Exit, as agreed between Parties under the Agreement;

23. **Processing** as defined in Article 2(7) Data Act. For easy reference) being: 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;

24. **Provider** (or as also mentioned in Article 2(34) Data Act, **Source Provider)** means the source provider of data processing services being the legal entity with whom Customer wishes to enter into, enters into or has entered into a legal relationship regarding providing data processing services and other Services by Provider under the Agreement;

25. **Same Service Type** as defined in Article 2(9) Data Act. For easy reference) being: a set of Data Processing Services that share the same primary objective, data processing service model and main functionalities;

26. **Services** means both the Data Processing Services as well as all Other Services as agreed by Parties under the Agreement;

27. **Service Fee** means the fees due and owed by Customer to Provider as consideration for the provision of Services as agreed by Parties under the Agreement;

28. **Switching** as defined in Article 2(34) Data Act. For easy reference : the process involving the (source) Provider, a Customer of a data processing services 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;

29. **Switching charges** as defined in Article 2(36) Data Act. For easy reference: 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.

### Info points - General

*The Data Act itself also caters for additional possibilities, being (A) Customer and the Provider have access to a dispute settlement body designated by Member States in accordance with Article 10.4 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) Data Act.*

*However, please do note that the Member States define the tasks and powers of the competent authority designated by the relevant Member State, and these may vary to a certain extent. It is therefore possible that such authority is not competent to settle disputes between the Customer and the Provider. The Parties must, therefore, assess the most appropriate way to oblige the other party to fulfil its legal and contractual obligations, and how to settle disputes.*

**Standard contractual clauses (SCCs)**

**for Data Processing Services**
including without limitation: cloud computing services

**SCCs Switching and Exit**

**Background – switching between cloud service Providers**

**The Data Act's main aims 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 on-premise ICT infrastructure; or (iii) make use of multiple services from different providers simultaneously. Therefore, the Data Act specifies the obligations of the source Provider which should make it possible. Even so, the Customers should also assess their goals related to switching and, in particular, specific needs, additional expenditures or timing. Both the Source Provider, the Customer and Destination Provider shall 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.

**The Data Act requires Providers to provide Customers with a written contract setting out the switching process when moving to another Provider or from cloud to on-premises infrastructure**. Terms must also cover timelines for switching (Maximum Transitional Period of 30 days) and details of any costs involved (including termination fees and egress charges). There are also obligations in relation to the switching process itself. These include 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.

**The switching charges:** As per the Data Act, 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 (Article 29). For switching after 12 January 2027, the Provider is not allowed to request switching charges. The switching charges for instance also include costs of automated switching tools or testing tools or assistance in the scope agreed with the customer.

Where a data processing service is being used in parallel with another data processing service, the Providers may pass on egress costs incurred to the Customer (Article 34), otherwise, the data egress charges will be regarded as switching charges.

**Professional services required by the switching process:** Article 25(2)(a)(i) of the Data Act specifies that "*... the provider shall... (i) provide reasonable assistance to the customer and third parties authorised by the customer in the switching process."* This "reasonable assistance" is part of the switching charges that will be eliminated over time as mentioned in Article 29. The labour time is highly dependent on the quality of the tools provided. If the Provider does not want to provide a lot of man-days of professional services for the support of Customer's switching process, the Provider has to provide an efficient and easy-to-use tool to export and transfer the Data and Digital Assets outside of its environment. This can drastically reduce the volume of professional IT services required by the switching process. The cost of the professional IT services required to import and implement the solution in the environment of Destination Provider will be borne by Customer.

The Data Act specifies cases where a standard approach is not possible:

- Article 29(5) stipulates *"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): " *... providers ...shall make the information ...publicly available*..".

**What should these Provider's switching and exit contract terms look like?**

**The standard contractual clauses on switching and exit provided here are intended to be a model for best practice, putting into effect the obligations to have a contract as set out in the Data Act. These are recommended clauses for use by the Parties.** They are intended to give you concrete examples of what should be included in the switching and exit contract terms, especially if you have never seen this type of clause before. There is no legal obligation to use these clauses and you are free to vary them because they are intended to help the parties to agree fair and reasonable contract terms. You have the right to negotiate the contract before signing it.

**What is included in these Switching and Exit terms?**

**Definitions**

To understand the terms used in these standard clauses, we recommend that you consult first the SCC General, Annex 'Definitions', applicable for all SCCs. Key terms in these SCCs are defined there and start with a capital letter.

**Exceptions:**

Please note that the Data Act provides for certain **exceptions** to certain obligations related to **SCCs Switching & Exit**. For instance, in accordance with Article 31 Data Act exemptions apply 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,

B. **AND** those data processing services are not offered at broad commercial scale via the Provider's service catalogue,

C. **AND** where the Provider has duly informed the Customer of these particular services before the Agreement/contract is concluded.

For such custom-built or highly individualised services, the Customer's right to switch continues to apply, but the parties need to agree on how (including the cost) such switching could take place.

Depending on the particular exemption, certain legal obligations may not apply. However, it is up to the negotiations between the Customer and the Provider whether to include these in their Agreement/contract. 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 duly inform prospective customers, well-before the conclusion of an Agreement, about specific services to which the switching obligations laid down the Data Act do not apply.

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, and the related SCCs below.

**Switching scenarios**

There are different types of data processing services. An increasing number of Providers offer self-service switching tools for both data ingress when you start using a service, and data egress when you stop using a service and switch either to an on-premise system or to a new (Destination) Provider. For some services, there may not be such tools, or they may not enable complete switching. Below we present basic two approaches for planning the switching and exit: (i) switching with the use of automated tools and (ii) switching based on the switching and exit plan. These options are not exclusive of each other and may be combined (for example, in the switching and exit plan in an annex, the parties may also envisage the use of automated tools which may apply for some service types or some data).

In both scenarios the Providers have obligations to remove obstacles to effective switching. Some are laid out in Article 26(a) "*The provider of data processing services 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";*
*and Art 30(1)….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".*

**Is the Data Act applicable for any model of cloud services (e.g. to PaaS or SaaS contracts)?**
**Yes,** these SCCs are applicable to all types of models of cloud services contracts (in particular for PaaS or SaaS contracts).
Article 30 "Technical aspects of switching" makes the difference between:

1. *Providers of 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* …. - This defines clearly IaaS

*and*

2. *Providers of data processing services, other than those referred to in paragraph 1,….*
   *This also includes, amongst other Data Processing services, such as PaaS and SaaS*

Recital 81 of the Data Act specifies that the generic concept "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.

**Are there differences between IaaS, PaaS and SaaS ?**

In IaaS the Provider does not know the content of the data nor the structure of the data and digital assets. The Customer uses the IaaS as servers, CPU (Central Processing Unit), memory, disk space and network lines to run his data processing services.
In PaaS and SaaS, the Provider does not know the content of the Customer's data . These data will eventually be encrypted. Yet, the Provider must know the structure of the database to provide services such as space allocation, optimization, reorganization and backups. Thus, without knowing the Customer data, the Provider can develop tools to export and transport Exportable Data. For example, each data table can be exported as a flat file with the corresponding metadata. The Providers of IaaS,

PaaS and SaaS have an important role during the switching process because they must allocate sufficient resources (servers, CPU, memory, I/O, bandwidth…) for a successful switching process.
***Info Point 1***

**Clauses**

The clauses are drafted so that it is clear what happens and when, and who has the relevant contractual obligations, including the timings, during the switching and exit process.

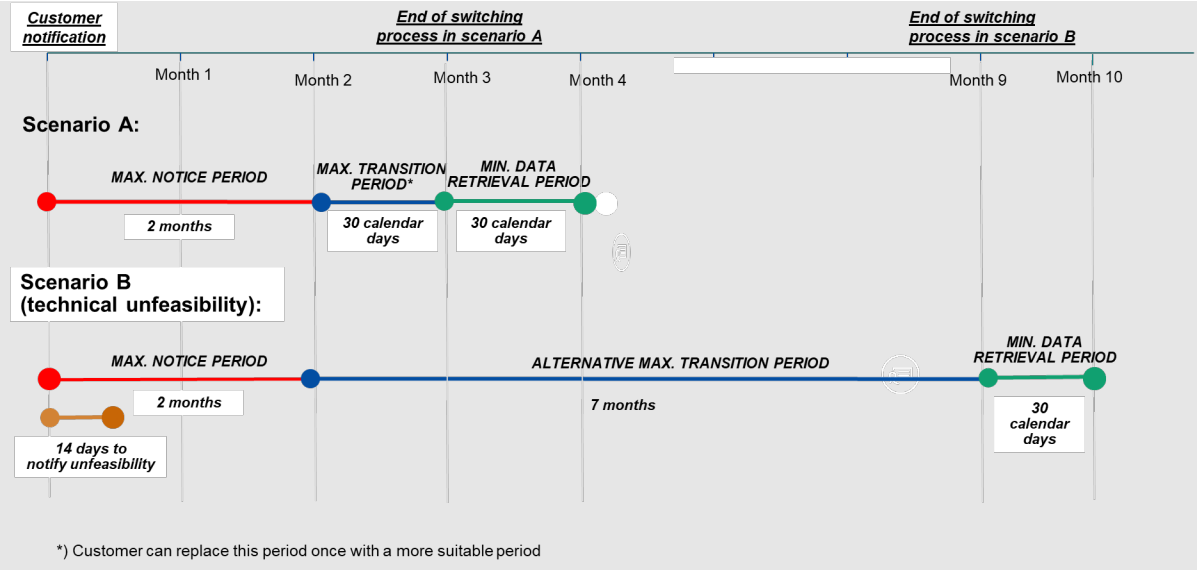
**Clauses on actions during the Maximum Notice Period and Transitional Period**

**Initiating switching.** The Data Act requires that contracts provide for a **Maximum Notice Period** for initiating the switching process, which must not exceed **2 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 Periods**. The Data Act requires that contracts include provision 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 no longer than the **mandatory Maximum Transitional Period of 30 calendar days starting with the end of the Maximum Notice Period**.

The Data Act also requires that the contract contain **a Minimum Period of Data Retrieval of at least 30 calendar days**, starting after the termination of the transition period.

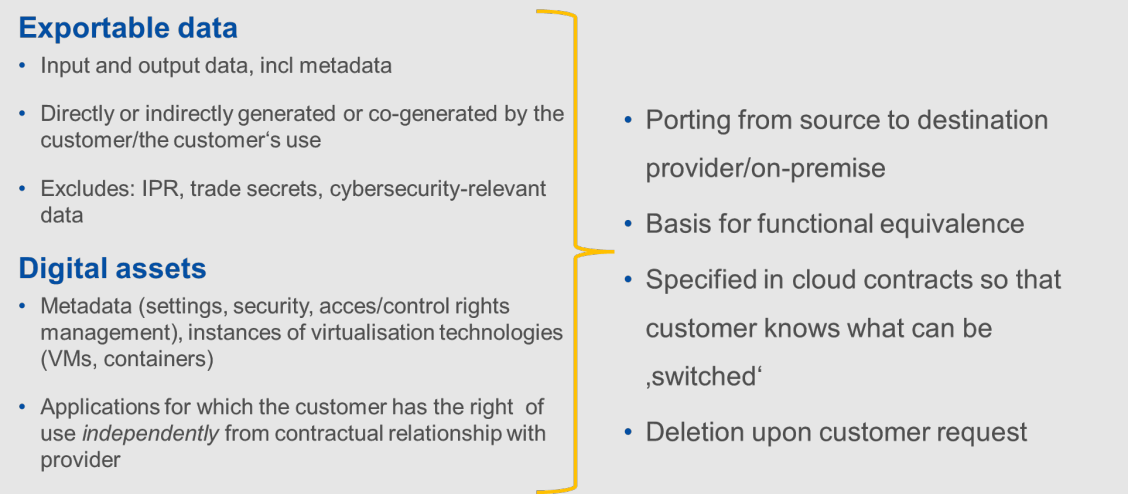
Where the **Maximum 30-day Transitional** Period for switching is technically unfeasible, the Provider must notify the Customer within 14 working days after the switching request has been made, explain the technical unfeasibility, and indicate an **alternative Transitional Period, which may not exceed 7 months**. The Customer has the right to extend the Transitional Period once, by a period that the Customer deems more appropriate.




The data processing agreement is considered terminated upon completion of successful switching or at the end of the Maximum Notice Period, if Customer does not want to switch but to erase its exportable

data and digital assets upon service termination. **No termination notice from Customer is needed, as the Agreement will terminate automatically.** The Provider is obligated to notify the customer of contract termination (Art. 25(2)(c) of the Data Act).

**What will be switched?**




**Option A: Switching and exit plan as an Annex to the Agreement**

We recommend that, especially in case of complex data processing services, Parties consider before concluding the contract a detailed plan for switching and exit. The switching and exit plan is intended to give parties a clear vision from the beginning of the relationship with the Provider on the switching process, and 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 Customer's services or business.

**Examples when the switching and exit plan may be useful**
**Example**: A SaaS system used to manage a warehouse of car spare parts with more than 100.000 different references from 1.000 different suppliers and picking of 10.000 items daily. How should the sequence of export be defined? What will be the timing?
**Example**: An insurance broker with 5.000 customers, 8.000 contracts, 1.200 claims, 10 employees, 10.000 (historical) agenda items and 200.000 (historical) documents. How should the sequence of export be defined and how will be the timing?

The switching and exit plan template in the annex is only an example of a such a plan that gives the Customer some idea of what questions they will need to ask their Provider and how to structure those discussions.
The division of responsibilities during execution of the switching process is an example, and the parties may agree to regulate it differently and in greater detail.

For this reason, the plan is unlike a standard contract term. One option is to keep it as a separate technical Annex to the contract, to be amended and updated by the Parties separately. Alternatively, the Parties may want to make the Annex part of the contract itself if they find that this makes it easier to enforce or update it. This is the Parties' choice and depends on how they organise and manage their contracts.

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.

We recommend that the switching and exit plan be updated during the Agreement as required by the evolution of the Data Processing Services and the data covered by the Agreement, and at least regularly, at a time interval agreed by the parties.

This update could also affect the agreed transitional period – for example, within the limits set by the Data Act (see the information provided in the explanatory notes for users of the SCCs on switching and exit).

This Annex would be useful only for exportable data if the customer switches providers and exits the current agreement and not if the Customer initiated the process with a request to have their data deleted at the end of the notice period (i.e. when the data is not transferred).

**Option B: Self-service automated switching tools**

Though it is more and more popular, such automation may come with some challenges. A particular concern is that in SaaS model, some databases and their setups may not be migrated properly and/or completely, triggering the need for manual intervention by the Provider. In case the Provider relies on such a self-service solution, these clauses (Option B) allow the Customer to make sure in the Agreement that sufficient information about the process and the tool itself is made available. The elements included in Option A (Switching and exit plan as Annex to the Agreement) may serve as inspiration in this respect.

**Standard Contractual Clauses on Switching and Exit**

**Option A: Switching and exit with a plan as an Annex to the Agreement**

## 1. Information

1.1. Before placing the order for the Data Processing Services, the Provider has provided the Customer with clear information about:

1.1.1. their standard service fees and, where applicable, early termination penalties;

1.1.2. the Switching Charges;

1.1.3. 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;

1.1.4. specific services where the obligations on switching and exit do not apply, where relevant.

***Info point 2:*** *Article 31 of the Data Act*

***Info point 3:*** *Article 30(6) of the Data Act*

1.2. Annex […] to the Agreement includes:

1.2.1. an exhaustive specification of Categories of Data and Digital Assets that can be transferred, including at a minimum all Exportable Data;

1.2.2. 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 obligation to export data where there is a risk of breach of the Provider's trade secrets.

***Info point 4***

1.2.3 clear information concerning known risks to continuity in the provision of the functions or services on the part of the source Provider.

1.3. The Provider's on-line register with data structures and formats, relevant standards and open interoperability specifications for Data is available at [….].

## 2. Switching and Exit Plan

2.1. The Parties agree on a switching and exit plan (the "Plan"), which will be included as an Annex to the Agreement and will be implemented by the Parties. The Plan must include:

2.1.1. details regarding switching and exit assistance, including the porting methods and formats, and steps required to carry out the switching process;

2.1.2. the contact designated respectively by the Customer and the Provider to carry out the Plan;

2.1.3. an estimate of the time needed to export and transfer the Data and Digital Assets out of the source Provider's environment;

***Info point 5***

2.1.4. restrictions and technical limitations, including those arising from storage of Data outside of EU;

2.1.5. a description of the sequence of operations proposed by the Provider;
2.1.6. a description of the testing method proposed by the Provider if tests are carried out.

2.2. If required by the Customer, the Provider must provide information explaining relevant procedures to the Customer's designated personnel (or such other third parties as the Customer may authorise)

2.3. If requested by the Customer, the Provider either will undertake to arrange a test or will support Customer in its testing, 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.

2.4. The Provider and the Customer undertake to update the Plan whenever necessary and at least to check, at the Customer's request, if changes are required.

***Info point 6***

**3. Initiation of the switching process**

3.1. The Customer must give the Provider a switching notice that it initiates the switching, observing the Notice Period. If the Customer wishes to switch only with regard to certain Services, Data or Digital Assets, it must specify that in the notice. The examples of such notices are stated in Annex [2a and 2b]

***Info point 7***

3.2. In such switching notice the Customer may inform whether it intends:

3.2.1. to switch to a different Provider of Data Processing Services. In this case the Customer should provide necessary details of the Destination Provider;

3.2.2. to switch to an on-premises ICT infrastructure of the Customer; or

3.2.3. not to switch but only erase their exportable Data and Digital Assets.

3.3 The Provider should confirm to the Customer the receipt of the switching notice not later than [within 3 working days] using the same way of communication as the one used by the Customer.

**4. Transitional Period**

4.1. When the Provider cannot respect the agreed [mandatory maximum] Transitional Period because this is not technically feasible, the Provider undertakes to:

4.1.1. notify in writing including by adequate electronic means, the Customer within 14 working days after receiving the notice for switching;

4.1.2. indicate an alternative Transitional Period, which must not exceed seven (7) months from the date of the Customer's switching notice; and

4.1.3. give proper justification for the technical unfeasibility.

The Customer should then confirm the receipt of such extension notice [within 3 working days].

4.2. The Customer may extend the Transitional Period once, for a period they consider more appropriate for their own purpose, for no longer than [xx months]. In that case, the Customer must notify 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 should confirm the receipt of such extension notice [within 3 working days].

## 5. Obligations of the Provider during the switching process

5.1. The Provider undertakes to provide reasonable assistance to the Customer and third parties authorised by the Customer once the switching process starts and throughout its duration so that the Customer can switch within the Mandatory Transitional Period. To this effect, the Provider must, in particular:

5.1.1. Provide capabilities, adequate information (including documentation necessary to complete switching) and technical support. If problems are detected, the Provider and the Customer will in good faith analyse the causes and agree on solutions.

5.1.2. Act with due care to maintain business continuity and continue to provide the functions or services under the Agreement .

5.1.3. Maintain a high level of security throughout the switching process, in particular for the security of the data during their transfer.

## 6. Customer's obligations

6.1. The Customer undertakes to take all reasonable measures to achieve effective switching. The Customer undertakes to be responsible for the import and implementation of Data and Digital Assets in their own systems or in the systems of the Destination Provider.

6.2. The Customer or third parties authorised by them, including the Destination Provider, undertake to respect the intellectual property rights of any materials provided in the switching process by the Provider, as well as Provider's trade secrets. The Customer undertakes to provide access to and if necessary to sublicense the use of these materials to third parties or to the Destination Provider only insofar as necessary to complete the switching process until the end of the agreed Transitional Period, including the alternative Transitional Period, respecting at the same time the confidentiality commitments, as well as the intellectual property rights granted by the Provider.

***Info point 8***

## 7. Data retrieval and erasure of data

7.1. The Customer could retrieve or erase their data during the agreed Period of Data Retrieval, which is […] days.

7.2. At the end of the agreed Retrieval Period, 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 personal Exportable Data which the Provider is obligated to store under EU or local laws.

***Info point 9***

## 8. Charges for the switching process and egress charges

The charges to be paid by the Customer for switching are as follows…

***Info point 10***

## 9. Termination of the switching process

9.1. As soon as the Customer notifies the Provider that the switching process is successfully completed, the Provider undertakes to notify the Customer immediately of the termination of the Agreement. This corresponds to Clause 5.1 in the SCCs on Termination. [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 whether the successful switching took place. If the Customer will not confirm successful switching within 30 working days from such request, it is deemed that the switching was not successful and the Agreement will not be terminated and will continue on its existing terms.]

9.2. If the Customer does not want to switch but to erase their Exportable Data and Digital Assets, at the end of the agreed Notice Period the Provider undertakes to notify the Customer of the termination of the Agreement. *See Cl. 6.2.3 of SCC Termination*

***Info point 11***

**Option B:** Switching and exit with **Self-service automated switching tools**

## 1. Information

1.1. Before placing the order for the Data Processing Services, the Provider has provided the Customer with clear information about:

1.1.1 available self-service automated switching tools for such Services ("Switching Tools") and the conditions of their use;

1.1.2 their standard service fees and, where applicable, early termination penalties;

1.1.3 the Switching Charges, including the fees for use the switching tools;

***Info point 12***

***Info point 13***

1.2. Annex [to option B] to the Agreement includes:

1.2.1. an exhaustive specification of categories of Data and Digital Assets that can be transferred with the use of Switching Tools, including at a minimum all Exportable Data;

1.2.2. 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 obligation to export data where there is a risk of breach of the Provider's trade secrets.

1.2.3. 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 storage of Data outside of EU, procedures, instructions, 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 the Customers during the switching or alternative communication channels, tests scenarios. This information must explain how to switch all Exportable Data and Digital Assets in a coherent and consistent way fast enough for an effective switching.

1.2.4. 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;

1.2.5. clear information concerning known risks to continuity in the provision of the functions or services on the part of the source Provider;

1.2.6. the resources, such as servers, CPU, memory, I/O, bandwidth ("IT Resources") which will be ensured by the Provider for an effective switching and the procedure for obtaining additional IT Resources, if required by the Customer.

1.3. The Provider's on-line register with data structures and formats, relevant standards and open interoperability specifications for Data is available at [….].

## 2. Initiation of the switching process

2.1. The Customer must give the Provider a switching notice that it initiates the switching, observing the Notice Period. If the Customer wishes to switch only with regard to certain Services, Data or Digital Assets, it must specify that in the switching notice. The examples of such notices are stated in Annex [2].

***Info point 14***

2.2. In the switching notice the Customer may inform whether it intends:

2.2.1. to switch to a different Provider of Data Processing Services; in this case The Customer should provide necessary details of the Destination Provider;

2.2.2. to switch to an on-premises ICT infrastructure of the Customer; or

2.2.3. not to switch but only erase their exportable Data and Digital Assets.

2.3 The Customer may also indicate in the switching notice the time window(s) for switching (i.e. a period, for example a weekend, during which the Customer intends to make its systems unavailable for the users and no update occur so that the data are frozen and Customer may carry out the 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 [3 working days] of notice with due justification and propose several alternative "time-windows" to the Customer ensuring at the same time that the Maximum Transitional Period is respected.

2.4 The Provider should confirm to the Customer the receipt of the switching notice not later than [within 3 working days] using the same way of communication as the one used by the Customer.

***Info Point 15***

## 3. Transitional Period

3.1. When the Provider cannot respect the agreed [mandatory maximum] Transitional Period because this is not technically feasible, the Provider undertakes to:

3.1.1. notify in writing including by adequate electronic means, the Customer within 14 working days after receiving the notice for switching;
3.1.2. indicate an alternative Transitional Period, which must not exceed seven (7) months from the date of the Customer's switching notice; and

3.1.3. give proper justification for the technical unfeasibility

The Customer should then confirm the receipt of such extension notice [within 3 working days].

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 [xx months]. In that case, the Customer must notify 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 should confirm the receipt of such extension notice [within 3 working days].

## 4. Obligations of the Provider during the switching process

4.1. Provider undertakes to provide reasonable assistance to the Customer and third parties authorised by the Customer once the switching process starts and throughout its duration so that the Customer can switch within the Mandatory Transitional Period. To this effect, the Provider must, in particular:

4.1.1 Act with due care to maintain business continuity and continue to provide the functions or services under the Agreement .

4.1.2. Maintain a high level of security throughout the switching process, in particular for the security of the data during their transfer.

4.1.3. 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.

***Info Point 16***

## 5. Customer's obligations

5.1. The Customer undertakes to take all reasonable measures to achieve effective switching. The Customer undertakes to be responsible for the import and implementation of Data and Digital Assets in their own systems or in the systems of the Destination Provider.

5.2. The Customer or third parties authorised by them, including the Destination Provider, undertake to respect the intellectual property rights of any materials provided in the switching process by the Provider. The Customer undertakes to provide access to and if necessary to sublicense the use of these materials to third parties or to the Destination Provider only insofar as necessary to complete the switching process until the end of the agreed Transitional Period, including the alternative Transitional Period, respecting at the same time the confidentiality commitments, as well as the intellectual property rights granted by the Provider

***Info point 17***

## 6. Data retrieval and erasure of data

6.1. The Customer could retrieve or erase their data during the Agreed Period of Data Retrieval, which is […] days.

6.2. At the end of the Agreed Retrieval Period, 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 it will retain, for how long and on what grounds.

***Info point 18***

## 7. Charges for the switching process and egress charges

The charges to be paid by the Customer for switching are as follows…

***Info point 19***

## 8. Termination of the switching process

8.1. As soon as the Customer notifies the Provider that the switching process is successfully completed, the Provider undertakes to notify the Customer immediately of the contract's termination. This corresponds to Clause 5.1 in SCCs Termination. [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 whether the successful switching took place. If the Customer will not confirm successful switching within 30 working days from such request, it is deemed that the switching was not successful and the Agreement will not be terminated and the Agreement will continue on its existing terms]

8.2. If the Customer does not want to switch but rather to erase their Exportable Data and Digital Assets as per point 3.2.3 *Initiation of the switching process* above, at the end of the agreed Notice Period the Provider undertakes to notify the Customer of the termination of the contract.

***Info point 20***

## Annex 1 for option B (referred to in Clause 1.2)

Either the information required is explicitly mentioned hereunder or the information required can be found at […..]

1. **Categories of Data and Digital assets that can be transferred including at a minimum all Exportable Data: ...**

1. **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 : ....**

2. **Data and Digital Assets protected by the intellectual property rights of Provider or third parties, which are exempted from switching: ....**

3. **Information on procedures for switching and porting with the use of switching tools:...**

4. **Estimate of the time needed to export and transfer the Data and Digital assets: ....**

**5. Known risks to continuity in the provision of the functions or services of the Source Provider: ...**

**6. IT Resources which will be ensured by the Provider for an effective switching:....**

**Annex 2 for option B (referred to in Clause 2.1)**

***Annex 2a – applicable if customer wants to switch***

*[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*]

On behalf of the Customer, I/we inform you that the Customer initiates switching of the Switched Services as of [starting date]. The notice period is [the customer to specify: maximum 2 months, may be shorter at the Customer discretion].

[*Optional wording*:

The Customer informs you that it intends to switch to [*details of new provider/on premise infrastructure of Customer*].

For automated switching. The Customer would like to switch in the following time window(s): [provide dates and details]. The Customer requests following IT Resources to be available in 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]

***Annex 2b – applicable if Customer does not want to switch but only to erase its exportable Data or Digital Assets***

*[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*]

On behalf of the Customer, I/we inform you that the Customer initiates switching consisting solely on erasure of Erased Data/Digital Assets as of [starting date]. The notice period is [the customer to specify: maximum 2 months, may be shorter at the Customer discretion].

*[Optional wording:*

Contact details of person responsible for switching: [details of Customer's representative responsible for switching process.]

_____

[signature of Customer's authorized representative]

*Annex to the Agreement (Option A)– Switching and Exit Plan*

**1.** Contact persons

- Provider's contact for switching and exit: …
- Customer's contact for switching and exit: …

**2. The Customer must provide the following information in the written notice:**

- Data concerned by the Notice, according to the agreed identification in the Annex on Data
- Destination of the Data: Customer's on-premises ICT infrastructure or a Destination Provider, including relevant technical specifications about the destination site.
- 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:

- confirmation of categories of data to be transferred during the switching process (2.1)

  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 ….

  Digital Assets:
  - L, in format ….
  - M, in format …..

- Provider's list of categories of data that are exempted

  - Categories of Data specific to the internal functioning of the Providers' data processing service where a risk of breach of the Provider's trade secrets exists: ...
  - Data and Digital Assets protected by intellectual property rights of Providers or 3rd parties : ...
  - Data and Digital Assets constituting trade secrets of the Provider or 3rd party :...

**4. Confirmation of the data to be switched**

The Customer will reply 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:

- The agreed order and timing for exporting and transferring the chosen Data and Digital Assets is as follows: …..
- Description of the testing method proposed by the Provider: ....
- The Provider or the Customer using the Provider's tools and processes will test the export and transfer to the agreed location with a part of the agreed Data and digital assets, to confirm or adapt the order and timing.
- The Customer will test the import and implementation of the agreed Data and Digital Assets in their own systems or the systems of the Destination Provider.
- 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**

- 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 and implement the Data or Digital Assets into their own systems or in the systems of the Destination Provider.
- The Customer (or any third parties the Customer has authorised) must test the functionalities in their environment or the environment of the Destination Provider 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.
- 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 is successfully completed, the Provider undertakes to notify the Customer immediately of the contract's termination. [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 whether the successful switching took place. If the Customer will not confirm successful switching within 30 working days from such request, it is deemed that the switching was not successful and the Agreement will not be terminated.]

## Info Points – Switching and Exit

***Info point 1:***

*In practice the situation is different in case of IaaS, PaaS and SaaS: Among other elements, the 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.*

***IaaS**: The Customer knows the structure of the database that he has defined. The IaaS Provider does not know the structure of the database.*

*The IaaS Provider must give details regarding the porting methods and, where appropriate, the necessary tools,*

*The Customer will define the sequence of operations, a time window (1) and the required IT resources.*

*The Provider must confirm the availability of the required IT resources during the time window.*

*The Customer initiates the switching at the agreed time.*

*The Customer is responsible for importing and implementing the data in the destination environment.*

***PaaS***

*The Customer knows the structure of the database that he has defined.*

*The PaaS Provider also knows characteristics of the database because the Customer asked him to provide services such as space allocation, optimization, reorganization and backups.*

*The PaaS Provider has a practical experience of the procedures for operations such as backups. He knows the resources required and the elapsed time*

*The PaaS Provider must give details regarding the porting methods and, where appropriate, the necessary tools and information and information about the timing and required IT resources.*

*The Customer defines the sequence of operations, a time window (1) and the required IT resources.*

*The Provider must confirm the availability of the required IT resources during the time window.*

*The Customer initiates the switching at the agreed time.*

***SaaS***

*The Customer doesn't know the structure of the database.*

*The SaaS Provider is the one who knows the structure of the database that he has defined.*

*The SaaS Provider knows the procedures and the time required for operations like backups, optimizations and reorganizations.*

*Moreover in case of installation of a new version of the SaaS software with a new version of the structure of the database, 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 on the procedure, resources and time required to export the data.*

*The SaaS Provider must 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 must agree on the sequence of operations, the time window (1) and the required IT resources*

*The Provider must 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 in the destination environment.*

*(1)time window: a period, for example a weekend, during which the Customer intends to make its systems unavailable for the users and no update occur so that the data are frozen and Customer may carry out the switching.*

***Info Point 2:*** *Article 31 of the Data Act lays down specific regime for certain Data Processing Services. For custom-built or highly individualised services, the Customer's right to switch continues to apply, but the Parties would 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 shall 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.*

***Info point 3:*** *According to Article 30(6) of the Data Act Providers will not be required to develop new technologies or services or disclose or transfer to a Customer or 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.*

*However, under Article 25 (1) of the Data Act, the rights of the Customer and the obligations of the Provider of data processing services in relation to switching must be clearly set out in a written contract, in particular with respect to the limits of the switching process.*

***Info Point 4****: Article 25.2(e) of the Data Act requires that the contract includes an exhaustive specification of all categories of data and digital assets that can be ported during the switching process. The Provider should define categories of data in a way that allows for evolution of the content into the defined categories.*

***Info point 5****:* ***Estimation of the switching time:*** *The Source Provider is responsible to estimate the time to export and transport the exportable data outside of its environment based on the time required to import the data, the estimated volume, network capacity and previous experiences or tests. The responsibility of the Customer is to estimate the time required to import and implement the data in the destination environment. Usually the volume of data used is available on the detailed reports available to customers (eg in the administrator's portal or similar tools). The customers/providers also have information about the services they use and the level of complication of such services.*

*There may be very different cases, this is why a switching and exit plan is important. The example of switching and exit plan includes an info point "Definition and execution of the switching process – Responsibilities for export".*

***Info point 6 on Clause 2.4*****:** *When you update the Plan, please check the SCCs on Non-amendment, in particular the clauses on 'Permitted Unilateral Change'.*

***Info point 7**: Subject to the terms of the Agreement, the Customer may choose only a certain subset of applications hosted by the Source Provider. In that case, the switching obligations concern only such applications and the corresponding Data and Digital Assets; for the rest, the previously agreed contractual terms still apply.*

***Info point 8:** 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.*

***Info point 9:** Data Retrieval starts after the agreed Transitional Period is terminated and must be at least 30 days after … (see Article 25(2)(g) of the Data Act and the SCCs on term and termination). The Customer does have the right to decide that it will not retrieve the data. In such case either it will erase it on its own (and may inform about it the Provider as stated in Article 25.3.(c) of the Data Act or the Provider will erase such non-retrieved data as stated in Clauses 7.2 of option A and 6.2 of Option B.*

***Info point 10**: If relevant, in the event of in-parallel use of a Data Processing Service (multi-cloud deployment scenario), the Data Egress charges will be agreed between the parties. The testing tools for switching and Provider's reasonable support of the Customer in testing as agreed in the Plan should be regarded as falling into switching process and consequently, the charges for such services should be gradually withdrawn in accordance with Article 29.*

***Info point 11**: It may happen that the switching process is not completed successfully and that the Customer's datasets / Digital Assets are not transferred, either completely or partially. In that case, all Parties involved must act in good faith and agree on the necessary measures to successfully complete the switching and exit process. In the event of failure of the switching process, the Data Processing Services continue to be provided and the Customer's data are not erased. SCCs on Termination section I of the Introduction and cl.1.3.*

***Info point 12:** The costs of using the Switching Tools provided by the Provider are the switching charges. Thus, after 12 January 2027, no fees for use of such switching tools will be allowed.*

***Info point 13**: Where a Data Processing Service is being used in parallel with another Data Processing Service, the Providers of such Services may impose Data Egress Charges. However, this is only to pass on egress costs incurred, without exceeding such costs, according to Article 34(2) of the Data Act. In this way, the Data Act accounts for multi-cloud deployment scenarios and allows the Provider to be fairly compensated for extracting their data through the network from the ICT infrastructure of a provider to the system of a different provider or to on-premise ICT infrastructure (such as outbound data transmission and the associated network traffic when workflows cross the respective cloud boundaries).*

***Info point 14**: The switching notice is a different instrument from contract termination notice. Subject to the terms of the Agreement, the Customer may choose only a certain subset of applications hosted by the Source Provider. In that case, the switching obligations concern only such applications and the corresponding Data and Digital Assets; for the rest, the previously agreed contractual terms still apply.*

***Info Point 15:** The Customer may need to carry out the switching in the specific time, to make it as little disruptive to its business as possible. 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 it intends 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 due to justified reasons (e.g." schedule maintenance of services which would severely affect the availability of resources during that time), it should provide the Customer with alternatives which would ensure effective switching by the end of the Maximum Transition Period.*

***Info Point 16**: Even in option B "self service automated switching tools" the Provider has its part of responsibility in 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.*

***Info point 17:** 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 to the switching 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. check the exported data and digital assets during the switching to immediately identify any problems).*
- *Appropriate contractual arrangements with the Destination Provider or ensuring appropriate resources for on-premises switching.*

***Info point 18:*** *Data Retrieval starts after the agreed Transitional Period is terminated and must be at least 30 days after … (see Article 25(2)(g) of the Data Act and the SCCs on termination).*

***Info point 19****: If relevant, in the event of in-parallel use of a Data Processing Service (multi-cloud deployment scenario), the Data Egress charges will be agreed between the parties.*

***Info point 20****: It may happen that the switching process is not completed successfully and that the Customer's datasets /Digital Assets are not transferred, either completely or partially. In that case, all parties involved must act in good faith and agree on the necessary measures to successfully complete the switching and exit process. In the event of failure of the switching process, the Data Processing Services continue to be provided and the Customer's data are not erased. SCCs on Termination section I of the Introduction and cl.1.3.*

**Standard Contractual Clauses (SCCs) for Data Processing Services**

including without limitation: cloud computing services

**SCCs Termination**

**Explanatory notes for users of SCCs Termination**

**Background: Termination of the Agreement in relation to a particular Service**

The Data Act enables customers of data processing services (including cloud and edge computing services) to switch between providers or to transfer their data to their own on-premises ICT infrastructure. To facilitate the implementation of the switching requirements under the Data Act, the Expert Group has drafted a set of standard contractual clauses ("SCCs") dealing with different aspects that are relevant for the switching process.

In particular, the SCCs below deal with the termination of the Agreement between the Customer and the Provider in relation to a particular service.

Please keep in mind that 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 with this specific service, unless the parties agree otherwise.

**What is included in SCC Termination?**

**Possible scenarios**

**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*). Clauses 4.1 and 6.1 lay out the cumulative conditions under which the termination will occur for each of those events. Please note that in such cases the Agreement will be considered terminated upon successful completion of switching (*Event A*) or et the end of the Maximum Notice Period (*Event B*). There will be no need to serve the termination notice or follow termination procedure from the Agreement, as the Agreement will terminate automatically. The Provider is however obligated to notify the Customer that the contract is considered terminated (Article 25.2(c). This notification is of informative nature, as the Agreement is already terminated. Thus, even if Provider delays the notification, it cannot charge any fee under terminated contract.

However, as the Provider may not be aware that switching was completed successfully, the Customer should inform the Provider about it. If the Providers has reasons to suspect that the Customer already successfully switched (e.g. the Customer is not logging into the service, 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 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 the switching is successful. In particular, to assess:

a. Completion of data transfer i.e. whether all exportable Data and if applicable, Digital Assets have been transferred to the Destination Provider's, as well as whether accuracy,

integrity and completeness of such was maintained. The exported Data and Digital Assets should match the original Data and Digital Assets and there should be no loss thereof and no corruption therein or related thereto.

b. Deployment of Digital Assets (if applicable). If switching included transfer of Digital Assets, such as 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 Destination Provider's service including switched Data or Digital Assets to assess whether its switching verification criteria are met.

In case of fixed term contract, the switching may end before the scheduled term of such contract or after that (for latter, see Event D). If the switching ends before the scheduled term, the agreement will also expire, however, there may be early termination penalties due in such case.

Please note that the Providers of Data Processing Services must not impose any obstacles (technical, pre-commercial, commercial, contractual, organisational) to switching and even if such obstacle exists, they must remove them.

***Reference to**: Articles 23 (a), 25.2(c) and 29.4 of the Data Act*.

**What if switching is unsuccessful?** Clause 3.1 caters for the situation that the switching is not successful by spelling out the escalation and related steps that the Customer (and its Destination Provider) and the Source Provider will need to take, in good faith, together with the Provider to achieve a 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 its exportable data to a specific server. The following scenarios could occur:

- The Source Provider does not propose effective tools and procedures for exporting and transferring all exportable data to the specific server;
- Data has been delivered to the specific server but the Customer or the Destination Provider are unable to upload the data properly.

Data seem to be correctly transferred to the specific server, but when trying to upload it in SaaS solution B, problems occur. This may be due to:

- the Source Provider if, for instance, data is transferred incompletely or is of bad quality; or
- the Customer or the Destination Provider – if, for instance, the tools and procedures for importing all data are not effective.

For a swift resolution of the situation where the switching is unsuccessful and the Agreement cannot be terminated (thus, obliging the parties to extend it), the Expert Group suggests submitting a complaint to the competent authority under the Data Act, so that it takes a decision. However, it should be understood that the parties can also use any legal means available under their jurisdiction (e.g. submitting a claim, requesting injunctions from civil courts, etc.) See SCC General, points 7 and 8.

**Two (2) other – optional – scenarios:** Clauses 7.1 and 8.1 are optional, and present two other possible scenarios for the Parties to consider. While not expressly mentioned in the Data Act, they are likely to occur and as such are included in the clauses to help the parties resolve them. These scenarios are:

- The Customer wishes to extend the availability of their data from the Source Provider or maintain the contract giving option for buying new services in place for a longer period, whether or not this is preceded by service switching or by a simple service termination without any switching; the Customer needs only a service of limited functionality i.e. ensuring availability of their data for this longer period or a contract in place to have the possibility to order new service (*Event C*).

In this case, as the data will be available through a service of limited functionality, the Provider and the Customer should conclude a new agreement for this additional service (see Clause 7.1 below) or amend the existing agreement or otherwise. In particular, the parties should agree on an Alternative Data Retrieval Period, which will start at the end of the Agreed Period of Data Retrieval. In case of general (framework) agreements the customer may wish to keep the contractual relationship in place to be able to buy fast new services without going through the contract conclusion process, which in larger organizations may be lengthy and quite complicated.

- A fixed-term contract expires before the switching process has occurred or has been completed (*Event D*).

***Examples for Event C***: The Customer has exported and transferred its data successfully from the Source Provider to the Destination Provider in whose environment the data was deployed successfully. Alternatively, the Customer decides to terminate the service with the Source Provider without subsequently migrating to another provider. The Customer, however, does not wish its data to be erased and rather prefers to have it backed up safely with the Source Provider extending beyond the agreed Data Retrieval Period.

Any such additional service enabled by the Source Provider does not prevent the termination of the original agreement and the provision of the service based on a new or amended agreement.

***Example for Event D (fixed-term contract)***: 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 the agreement with the Source Provider expires.

The parties should be aware that a **s**uspension of services may occur during the switching process. In this case, the general clause on suspension of services included in the Agreement applies.

**Termination under mandatory applicable law as indicated under Clause 2.1. below.** Clause 2.1 explicitly makes it clear that even in case of termination under a mandatory applicable law, the Agreement will be in force and the services and functions under the Agreement will continue in full until any of the events described under Clause 1.1 occurs.

**Exemptions for certain custom-built services exist:** Data processing services which are fully or partially (the majority of their main features) custom-built to respond to the specific demands of an individual customer are exempted from some – but not all – legal obligations applicable to switching. Services, which the Provider offers at a broad commercial scale, are however subject to the switching legal obligations. The Provider should duly inform prospective customers, well-before the conclusion of an Agreement, about specific services to which the switching obligations laid down the Data Act do

not apply. The parties can always agree in the Agreement to include switching provisions for such services, too.

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, and the related SCCs below.

These SCCs are also applicable to the above-mentioned services that are subject to exemptions, unless they are directly related to achieving functional equivalence in the use of the new Data Processing Service in the ICT environment of a different Provider of Data Processing Services of the same type.

**Standard Contractual Clauses on Termination**

**Definitions**

To understand the key terms used in these SCCs, we recommend that you first consult the section on "Definitions", which are applicable for all SCCs. The terms in this SCC starting with capital letter are defined in the section "Definitions".

**Termination**

1.1 The Agreement will be considered terminated between the Parties when one of the following events has occurred in full:

1.1.1 Where applicable, on the successful completion of the switching process ('*Event A*'). Should *Event A* occur before the agreed duration of the Agreement expires, then the early termination fees set out in this Agreement will apply, or;

1.1.2 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 on termination of the service ('*Event B'*).

Termination of the Agreement if the switching process is successfully completed, will be further detailed and otherwise arranged for in Clauses 4.1 and 5.1.

2.1 If the Agreement contains any terms regarding termination subject to statutory law or related cases such as those mentioned here below:

a. A Party is applying for moratorium, suspension of payments, or a Party has been declared bankrupt;

b. A Party has still not met, in a timely fashion, any material or other obligation arising from the Agreement that results or could result (either by contract or law) in a termination of the Agreement;

c. A Party has experienced a change of ownership or control that, by contract or law, results or could result in the 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. Similar or identical situations, or any other situations that, by contract or law, result or could result in the termination of the Agreement,

the Agreement together with the agreed Services and functions will not be terminated or expire before any of the situations described in the Clauses 1.1.1 or 1.1.2 (*Events A or B*) have clearly occurred. For the avoidance of doubt, this does not affect any other rights or remedies a Party may have available towards the other Party.

The Customer may agree its successful switching metrics, as well switching milestones with the Source Provider and report the status of their achievement during the switching process. In any

case, the Customer should inform the Provider of its successful switching as set forth in Clause 5.1.

3.1 If the completion of the switching process set forth in Clause 1.1.1 is not successful, Parties must cooperate in good faith to identify and resolve the matter at hand to improve the switching process and achieve successful completion, enable a timely transfer of data and maintain continuity of the Services. In particular, upon Customer request the Provider should support the Customer in identifying the reasons for unsuccessful switching and advise how identified obstacles could be removed or worked around. If the Customer relied on the automated tools offered by the Provider, which have not ensured successful switching, the Customer may demand that the Provider agree the detailed Switching and Exit Plan, as referred in SCCs on Switching and Exit to carry out the switching process within [xx] days from the Customer's request. The rules applicable to switching charges apply to support and other Provider's services referred to in this section.

3.1.1. At its discretion, Customer will involve the Destination Provider on Customer's behalf.

3.1.2. Without prejudice to other legal remedy available under applicable law, the Agreement will not be terminated or expire before successful completion of the switching process, or before a relevant decision taken by a competent court or by a between Parties chosen and agreed forum.

3.1.3. If there is any conflict or inconsistency between these Clauses and any other agreement on termination between the Parties, these clauses shall take precedence.

## I. Termination Process

4.1. Successful completion of the switching process set forth in Clause 1.1.1 can only occur and will be (deemed) completed, after:

4.1.1. the [Maximum] agreed Notice Period has expired, and

***Info point 1***

4.1.2. the Transitional Period has commenced after the Notice Period has elapsed, Clause 1.1.1 applies, and the Switching and Exit Assistance set out in that clause must be initiated and completed;

***Info point 2***

4.1.3. the Data Retrieval Period has commenced after the termination of the Transitional Period, and;

4.1.4. the data erasure has been completed successfully after the expiry of the Data Retrieval Period or after the expiry of an alternative agreed period following the successful completion of the switching process.

***Info point 3***

5.1. As soon as the Customer notifies the Provider that the switching process is successfully completed, the Provider undertakes to notify the Customer immediately of the termination of the Agreement. [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 whether the successful switching took place. If the Customer will not confirm successful switching within 30 working days

from such request, it is deemed that the switching was not successful and the Agreement will not be terminated and will continue on its existing terms.]

6.1. If the Customer does not wish to switch but rather to erase its Exportable Data and Digital Assets set forth in Clause 1.1.2 can only occur and will be deemed completed, if:

6.1.1. the [Maximum] agreed Notice Period has expired, and;
6.2.2. the Customer has unconditionally and clearly 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.
6.2.3. At the end of the agreed Notice Period the Provider undertakes to notify the Customer of the termination of the Agreement.

**Other Options** *[*Optional clauses to be considered]*

7.1. If at the end of the Transitional Period the Customer decides not to erase all its exportable data and digital assets at the end of the [Minimum]/Agreed Period of Data Retrieval and wishes to ensure that they will be available in the service of limited functionality for a specified additional time or the Customer and Provider agreed to maintain the Agreement in place without providing any specific services, unless ordered explicitly by the Customer (*Event C*), such can only occur, after:

7.1.1. the [Maximum] agreed Notice Period has expired, and;

7.1.2. the Transitional Period is completed, and;

7.1.3. an Alternative Period of Data Retrieval and other terms and conditions for the service of limited functionality or maintaining the Agreement in place have been agreed between the Customer and the Provider (in particular, allowing the Provider to delete the data after the Alternative Period of Data Retrieval, and/or specifying the remuneration for such additional term).

If the Alternative Period of Data Retrieval and other conditions of service during such time are proposed by the Provider, the Agreement must not terminate or expire before the Customer has (at their sole discretion) accepted the solution and unambiguously confirmed that the Agreement is terminated.

8.1. If the Agreement has been explicitly concluded for a fixed duration and the expiry date is reached before the switching process is completed, and the Customer has not requested its exportable data and digital assets to be erased (*Event D*), then:

8.1.1. the Transitional Period begins on the Agreement expiry date, and the Provider shall provide reasonable assistance as set out in SCC Switching and Exit;
8.2.2. on successful completion of the switching process, the Clauses 1.1.1 and 2.1 above applies (*Event A* is triggered), and;

8.2.3. on unsuccessful completion of the switching process, Clause 3.1 above applies .

## Info Points - Termination

***Info point 1****: Reference is made to SCC General, Annex Definition, Article 25.2(d) of the Data Act.*

***Info point 2:*** *Transitional Period as defined in the SCC General, Annex Definition, and set forth in clause 4 Option A and clause 3 Option B of the SCC on Switching and Exit for the possibility for it to be extended by either the Customer or the Provider.*

***Info point 3****: Data retrieval clause 7 in Option A and clause 6 in Option B the SCCs on Switching and Exit and Article 25.2(h) of the Data Act.*

**Standard Contractual Clauses (SCCs)**
**For Data Processing Services**
including without limitation: cloud computing services

**SCCs Security and Business continuity**

**Explanatory notes for users of the SCCs on Security and business continuity**

**Background**

The first sentence of Recital 94 of the Data Act reads:

'*Throughout the switching process, a high level of security should be maintained*.'

While the topics of security and business continuity are normally included in the services agreement, the Data Act focuses on the importance of security and business continuity with relation to the switching and exit process (collectively 'switching process'). In this context, the Data Act lays down obligations for the Provider to ensure a high level of security throughout said 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).

In order to do so, the high level of security already will need to be in place well-before the switching process, and at least to be sustained at that high level during the switching process.

The Data Act also obliges the Provider to act with due care to maintain business continuity and ensure the provision of the functions or services under the contract (Art. 25(2)(a) (ii). 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 (Art. 25(2)(a) (iii).

**Explanatory notes**

These standard contractual clauses (SCCs) combine clauses on specific issues of business continuity and security **throughout** the switching process. This approach is chosen 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. Furthermore, the same legal framework applies.

These SCCs use the term '**significant impac**t' in relation to both security and business continuity. It is highly recommended that before entering a services agreement with the Provider, the Customer assesses and maps such possible '**significant impac**t' related to the Agreement, the Customer's use of the services and the need for security and business continuity, especially during the switching phase (see Clauses 1.5 and 1.9).

The switching process involves **particular security risks** to which special attention needs to be given. Such risks include:

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 concerning and otherwise related to preparing for and executing an effective switching phase.

**Risk-based security and business continuity:** Where the SCCs provide for contractual arrangements, a risk-based, respectively 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 Provider to jointly identify, agree upon, implement and monitor the related measures and controls in order to ensure improved overall service resilience and integrity accessible to all Customers.

For instance, special attention and consideration will need to be given without limitation 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) and the like;

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, and the like.

The Provider should also 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 the same or similar to the structure and approach as set out in (i) Article 25 GDPR and Article 32 GDPR [Regulation - 2016/679 ] respectively; (ii) the NIS2 Directive [EUR-Lex)], (iii) the Cybersecurity Act (EU) 2019/881 and related (existing or upcoming) cybersecurity certification schemes.

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 respectively all-hazard-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, without limitation: 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.

**Business continuity risks:** ensuring business continuity throughout the switching process deserves special attention and consideration in a similar spirit to security. The same regulatory framework applies.

For instance, risks pertaining to business continuity 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 said services.

**Standard Contractual Clauses on Security & Business Continuity**

**General**

1.1. In accordance with applicable EU or national law, while providing the services the Provider undertakes to apply the most appropriate technical and organisational measures to ensure the level of security and resilience appropriate to the risks presented by the services and their intended and reasonably foreseeable use.

1.2. Furthermore, the Provider undertakes to avoid service disruptions and maintain continuity of the services. This includes having and maintaining adequate business continuity management that comprises, without limitation, 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.

**Security**

1.3. Further to clause 1.1, in accordance with the applicable EU and national law, 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 the continued security of the data during the retrieval period.

1.4. The Provider must implement appropriate technical and organisational measures to ensure that a level of security appropriate to the level of risks is maintained during the switching process. This includes, but is not limited to:

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; and

B. any other risks concerning and otherwise related to effective switching.

1.5. Such measures as laid down in clauses 1.1 and 1.3 must – for any service model and any deployment model – at least ensure, without limitation:

A. ongoing confidentiality, integrity, availability of the data and resilience of the services, exportable data 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 a physical, technical or organisational security breach, incident or similar event (collectively: 'incident'); and

C. continuous monitoring and regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the security of the services, of the exportable data and the digital assets.

1.6. The Provider must notify the customer of any incident that may significantly impact the Customer's use of the services, the Customer's exportable data and digital assets. The Provider must give the notification without undue delay – but in any event not later than 48 (forty-eight) hours from becoming aware of the incident, unless regulatory obligations require an early warning or similar notification within 24 (twenty-four) hours.
The Provider's notification must include the information required for the Customer to be able to thoroughly investigate the incident and related consequences. The Provider must promptly,

effectively, reasonably and at no additional cost, assist and otherwise 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.

***Info point 1***

1.7. The notification as referred to in clauses 1.6 and 1.10 must be made by the Provider to the Customer as follows:
[Parties to specify the mean(s) of notification. These may include – without limitation – a specific notification on the service portal used by the Customer, and/or via email to a contractually agreed email account of a duly authorised representative of the Customer regarding such notifications)].

1.8. Where the Provider is affected or is likely to be affected by an incident that may have an impact on the Customer's operations, including their ongoing use of the services, the provider must take the most appropriate action necessary to minimise the impact of such incidents and prevent these from recurring. This does not affect other rights that the Customer may have by Agreement or by applicable EU or national law.

**Business continuity**

1.9. Further to clause 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;

B. provide clear information concerning known risks to continuity in the provision of the services; and

1.10. The Provider must ensure that they notify the Customer as laid down in clause 1.6, without undue delay and not later than 48 (forty-eight) hours – unless regulatory obligations require an early warning or similar notification within 24 (twenty-four) hours – of any business continuity incidents or similar events (collectively: 'business continuity incident') that may have a significant impact on the Customer's use of the services, exportable data and digital assets. The deadline for the notification as indicated above starts from the moment the Provider becomes aware of any such incident.
The Provider must ensure that any such notification includes the information required for the Customer to be able to thoroughly investigate such event(s) and related consequences. The Provider must promptly, effectively, reasonably and at no additional cost assist and otherwise cooperate with the Customer (including with third-party suppliers of the Customer) regarding any investigation and action the Customer is entitled to undertake in accordance with applicable EU and national law.

1.11. Where the Provider is affected or is likely to be affected by a business continuity incident that may have an impact on the Customer's operations and the Customer's ongoing use of the services, the provider must take appropriate action necessary to minimise the impact of such events and prevent them from recurring. This does not affect other rights the Customer may have as provided in the Agreement or by applicable EU or national law.

**Miscellaneous**

1.12. 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, and of its business continuity and related contingency management and of any material changes to any of the above.

1.13. At the Customer's request, the Provider must without undue delay also 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 a non-disclosure arrangement to be concluded with the Customer before sharing such details. Such an arrangement 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.

***Info point 2***

1.14. Subject to the terms of the SCC Non-Amendment and SCC Non Dispersion, the Provider must as soon as reasonably possible make any changes to security measures and related security management, as well as to their business continuity measures and related contingency management as provided for in these SCCs, as necessary to ensure ongoing compliance as laid down in these two clauses.

## Info Points – Security and business continuity

***Info point 1:*** *An example of regulatory obligations to notify the Customer within 24 hours is NIS2, Article 23.4 '.. without undue delay and in any event within 24 hours of becoming aware of the significant incident.' However, the time windows mentioned above (24 respectively 48 hours) should not be read as a minimum. In security service level agreements for instance, shorter terms are not uncustomary, depending on the sector, risk classification and related possible impact.*

***Info point 2****: Such customary exceptions shall include, without limitation, any (relevant part of such) 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 or the like).*

**Standard Contractual Clauses (SCCs)**

**for Data Processing Services**

including without limitation: cloud computing services

**SCCs Non-Dispersion**

## Explanatory Notes for users of SCCs Non-Dispersion

### Background

The Data Act requires the providers of data processing services to remove contractual obstacles before switching to a new Provider or to an ICT premises. The Agreements for data processing services often comprise various other documents, which refer to additional materials and information, that can be widely dispersed across different repositories. This is a source of information asymmetry, limiting the trust between the Provider and the Customer and making it difficult for a prospective Customer to find all the information they need to assess the parties' contractual and legal obligations and their implications.

In the context of the switching process, transparency is also very important. A prospective Customer needs easy access to relevant, updated information, documents, materials and contact details, even before they conclude a contract with the Provider. The Data Act also stipulates the Provider's obligation to cooperate in good faith for the switching and to provide reasonable assistance to the Customer and third parties.

### Explanatory notes

Under Article 41 of the Data Act, these standard contractual clauses (SCCs) aim to enable and facilitate a fair contractual relationship between the Customer and Provider and help the Customer to negotiate with the Provider an appropriate level of transparency in the contractual conditions and their documentation.

It aims to create an environment of transparency between the parties, starting well before the Agreement is signed. The inclusion of this SCC in the Agreement ensures 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 fair and balanced legal relationships between the Customer and the Provider and, in general, to contractual fairness, as advocated by the Data Act.

For a Customer to know, at any given time during the duration of Agreement and even after its termination, which contractual conditions apply or used to apply, the Customer need to have easy access to accurate, complete and up to date documentation and information, which also includes performance reports, notifications and the like.

In this spirit, the relevant contractual documentation must be available at any time to give the Customer a quick and easy overview.

**Standard Contractual Clauses on Non-dispersion**

**Introductory conditions & arrangements**

1.1 The Provider undertakes that all contractual arrangements, as defined below, will be easily, readily and continuously findable, 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 manner. In addition, the Provider will ensure that the contractual arrangements are downloadable or otherwise exportable for the Customer in a complete and structured manner.

1.2 Contractual arrangements must include, without limitation:

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 then current, time-stamped (and where available execution copies of the) Agreement, including any and all terms, accepted offers, conditions, policies, information, documentation, schedules, exhibits, annexes or the like that are applicable between the Provider and the Customer;

c. **Historical overview:** the historical overview of the time-stamped Agreements, terms, conditions, including any policies, information, documentation, schedules, exhibits, annexes or other that have been applicable between the Provider and the Customer, including evidence of Permitted Unilateral Changes and the respective Permitted Unilateral Change Effective Dates.

***Info point 1***

d. **Data processing & supply ecosystem:** the then up--to--date as well as historical overview and detailed list of subcontractors (data processors and/or other relevant supply chain ecosystem stakeholders of the Provider, including names and addresses as in clause1.2 (a) above;

e. **Contact details:** the then 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, without limitation, the respective function titles, phone numbers and email addresses – or similar contact details proposed by Provider and accepted by Customer;

f. **Operational performance reporting:** an up--to--date as well as historical overview and details of the operational performance reporting by the Provider on the service provided and other obligations under the Agreement, in particular [*], and;

g. **Notification:** any and all legal and other relevant time-stamped notifications between parties or to a party concerning or related to the contractual arrangements as in clause 1.2 (a) and (b), above.

1.3 The Provider undertakes that all information rights that Customer has under the Data Act in general and these SCCs in particular will be met in a timely, accurate, correct, comprehensive, and, where possible, continuous manner. These information rights are further detailed in the respective SCCs.

***Info point 2***

1.4 To make the switching process effective, enable timely transfer of data and ensure the continuation of the services for the benefit of Customer, the parties must cooperate in good

faith. These cooperation rights are further detailed in the relevant, subject-specific chapters and paragraphs of these SCCs.

***Info point 3***

1.5 **Order of precedence.** These SCCs form an integral part of the Agreement. In the event of any conflict or inconsistency between these SCCs and any other applicable contractual arrangements, terms, conditions or other (parts of) applicable agreements – including any policies, information, documentation, schedules, exhibits, annexes or the like pertaining to them – these SCCs will take precedence.

## Info Points – Non-dispersion

***Info point 1***: *For Permitted Unilateral Changes and the respective Permitted Unilateral Change Effective Dates* see *SCCs Non-Amendment* [link]

***Info point 2***: *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) are included in SCCs Switching and Exit [link]; the obligation to provide clear information concerning known risks to the continued provision of functions/services is reflected in SCC Security and business continuity [link].*

***Info point 3:*** *See point A)d of SCC General.*

# SCCs Liability

## Explanatory notes for users of the SCCs on Liability

### Background

One of the main aims of the Data Act is to facilitate the switching process. To ensure that the switching is effective, the Data Act provides for the removal of obstacles, including contractual obstacles.

### How to achieve a more balanced relationship between the Customer and the Provider?

The Data Act recognises the importance of fairness in contractual relations, including those related to the cloud computing contracts and the switching process.

While the Expert Group acknowledges that a clause on liability is usually included in the general Agreement between the Customer and the Provider, it believes it is useful to include provisions on liability in the SCCs. In particular, small and mid-size companies and other organisations may find these SCCs helpful when they negotiate and/or draft liability provisions in their Agreements. The clauses also flag up issues that organisations, irrespective of their size, may not have thought of.

Before concluding an agreement, the Customer may check the insurance market for the most appropriate insurance product for their needs and for insurance cover specific to liability issues that may arise during the switching process. Seeking advice from an expert specialised in insurance is recommended.

During the switching process the responsibilities are shared between the Source provider, the Customer and, where relevant, the Destination Provider. The SCC Switching and Exit describes in detail the possible scenarios and the responsibilities of each Party.

### What is included in these liability terms?

#### The definitions

To understand the terms used in these standard clauses, we recommend you consult first SCC General, Annex 'Definitions' applicable for all SCCs [hyperlink].

**The explanatory notes** included in these SCCs provide more detail on the clauses and clarify certain drafting choices. They also provide explanations of the approach and logic for specific provisions (for example, the two approaches to limitation of liability, or why 'intent' and 'wilful' misconduct are separated). The explanatory notes describe exceptions to the obligations under Article 31 of the Data Act. They also draw Customers' attention to certain issues they should consider and avoid, as explained, e.g. in the note on the non-production environment.

#### The clauses

These SCCs are intended to give an example of liability clauses for fairer, more balanced, and non-discriminatory cloud contracts. The Customer and the Provider are also free to agree on additional rights and obligations in their contract, for instance in the case of services where the majority of the main features have been custom-built (see Article 31 of the Data Act). Likewise, the Customer and the Provider may include unlimited liability for breach of obligation to defend against third-party

intellectual property rights. They may also agree to increase the thresholds of certain liability of either party ('Party') or both parties to the Agreement ('Parties'), etc.

The parties can use the 'Annex to clause 4.6 Approach A' to these SCCs to clarify what they can include in a risk assessment before concluding the contract. The Annex suggests some risks that especially the Customer may consider.

**I. Definitions**

The key terms in these SCCs starting with a capital letter are defined in SCC General, Annex 'Definitions'.

**II. Explanatory notes**

1. **General rules of liability for breach of agreement:** As a rule, each Party to the Agreement should bear unlimited liability in cases of intent, wilful misconduct or gross negligence. The same applies where the Provider breaches confidentiality or obligations not to use data for purposes other than those agreed with the Customer. The SCCs recommend separating cases where the breach is intentional and where it is due to 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.
   *Reference to clauses 4.1, 4.2 and [Optional clause.4.3].*

2. **Confidentiality & non-use:** This clause ensures that the confidentiality of the Customer's data for generally available services is protected, and that the Provider is not allowed to use such data for their own purposes unless clearly agreed with the Customer. The Provider may wish to use certain Customer's data in order to provide the services as ordered by the Customers or to settle them (e.g. in pay as you use models). The Agreement should clearly indicate these rights of use – if any - and purposes of using said Customer data by the Provider, if and to the extent agreeable to Customer and such use complies to applicable law. If there is a breach of such obligations the Provider is fully liable.
   *Reference to clause 4.2 and [Optional clause 4.3].*

3. **Non-production environment:** Non-production versions of Data Processing Services for testing and evaluation purposes that are made available for a limited time, as provided for in Article 31(2) of the Data Act, are not intended for the processing of sensitive data (for instance, trade secrets, personal data or actual production data). Such non-production versions are 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 or sensitive data in such non-production versions. If the Customer decides to do so, this is at their own risk; the Provider cannot be held fully liable if a breach of data confidentiality occurs in such cases. In this situation, the liability arrangements agreed by the Parties will apply.
   *Reference to clause 4.4.*

4. **Other exceptions:** The Data Act envisages situations when certain switching obligations do not apply, i.e. for services where most of the main features have been custom-built, where all components have been developed for an individual customer, or for services provided in a non-production environment.
   *Reference to clause 4.5.*

5. **Limited liability:** It is current business practice that the parties agree to limit the Parties' (especially, Provider's) liability in some cases. In these SCCs, two main approaches for such limitations are proposed, being – in no particular order – certain limitations of the liability of a Party:

   **Approach A:** One Party is liable only for the risks identified together with the other Party based on risk assessment(s),

   **Approach B:** By means of a pre-agreed amount, annual fees, insurance or other formula.

   In principle, Parties should jointly opt for either Approach A or B. However, it is possible that only one Party' liability is set based on Approach A, while the other Party's - based on Approach B. In particular, Approach A may be easier to apply for the Customer to determine Provider's liability for breach of the Agreement.

   Approach B may be more commonly known and used. However, Parties are encouraged in any case to familiarise themselves with the Annex to Approach A so that they are aware of the risks related to data processing services for their particular business.

   *Reference to clause 4.6.*

   **Approach A:** Under this approach, each Party has to perform a risk/impact assessment and provide it to the other Party in the pre-contractual phase. The other Party has the right to reject the risk assessment received by the one Party but must give reasonable justification for doing so. If the risk assessment is rejected, Parties could consider Approach B.

   The Parties should keep in mind that where a service is provided within a contractual framework 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 the Party to revisit its risk assessment, with the Parties having to adapt the liability limit to reflect the actual risk situation.

   *Reference to clause 4.6 Approach A*.

   **Approach B:** This approach is based on limiting both Parties' liability to: (i) a pre-agreed amount and/or (ii) annual fees (paid and due) by the Customer to the Provider, (iii) the insurance coverage as taken out by Provider related to the Services , or (iv) a variety of other formulas.

   Under this approach, in a series of connected events considered as one event, the party's liability can be limited to aggregated liability for direct damage per one event. Here is a non-exhaustive list of examples of options that could be used in this case:

   a. a pre-agreed amount, e.g. 'EUR 500 000 (in words five hundred thousand Euro)';

   b. a formula linked to the services' monetary value, such as '[#] ([*numeric factor in words]) times the amount equal to the annual overall fees (either paid or (not yet) due under the Agreement) for the services';

   c. a formula linked to the Providers 's general professional liability insurance, such as 'the maximum amount as covered by the Provider general professional liability insurance'. The Provider will make such insurance policies and related documentation available for the Customer consideration before entering into the Agreement.

   *Reference to clause 4.6 Approach B*.

6. **Indemnification:** The SCCs on Liability below currently do not include an indemnification paragraph and clauses. It is however encouraged to consider whether and if so to what extent the party may need to undertake to indemnify and hold the other party harmless from any claims of third parties caused by or otherwise relating to a material breach of obligations under the

Agreement caused by acts or omissions of the liable party, its employees, representatives or Subcontractors. In case of Customers, the indemnification may apply, for instance to Provider's breach of its confidentiality obligations non-use or infringement of third-party's intellectual property rights. For Providers, the indemnification may cover the Customer's breach of third party's intellectual property rights or third party's claims to Provider related to hosting of illegal content by the Customer.

**Standard Contractual Clauses on Liability**

**A. *Unlimited liability***

4.1. In cases where the obligations under this Agreement is breached by a Party, in particular but not limited to breaches of the switching and related obligations or breaches of the confidentiality of the Customer's data, due to intent, wilful misconduct or gross negligence, such Party is liable for any and all damages, without limitation. The previous sentence is subject to clause 4.5.

4.2. The Provider is only allowed to use Customer data for purposes explicitly described in the Agreement, unless the Provider obtains the Customer's explicit written agreement to process such data for certain other purposes. In cases where said non-use obligation is breached, the Provider is liable for all damages, without limitation.

***[OPTION]*** *[*Optional clause to be considered; if parties opt for this clause this will also entail amendment of clause 4.1, while clause 4.4 could also then apply]*

*4.3. All Customer data processed under the Agreement must be qualified as confidential and are therefore subject to the confidentiality obligations as laid down in the Agreement. Except as stated in clause 4.4, in cases where such obligation is breached, the Provider is liable for all damages, without limitation.

***Info point 1***
***Info point 2***

***B. Waivers of unlimited liability***

*4.4. The provider's unlimited liability as stated in the [Optional] clause 4.3 does not apply to Customer data in a non-production version of the provider's data processing services. Non-production versions are intended for testing and evaluation by the Customer and are only made available to the Customer for a limited period of time.

***Info point 3***

4.5. The Provider is not liable for:

A. a breach of the Provider's obligations as set out in: (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) Data Act (technical aspects of switching). This applies in all cases (i) – (iii) only 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, provided that before the Agreement for such services is concluded, the Provider informs the Customer that the above-listed provisions of the Data Act do not apply to said services; or
B. a breach of the obligations set out in Chapter VI of the Data Act (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.

***C. Limited liability for any other breaches of the Agreement***

4.6. Except as otherwise set forth in the clauses 4.1 through 4.5, a Party:

***[Approach A: Liability cap: risk assessment or maximum amount]***

… is only liable in the event of a negligent breach of obligations under this Agreement. The liability for such negligence is limited to the amount determined by the aggrieved Party in good faith in a risk assessment it performed and provided to the other Party [in reasonable time] or [at least # days] before the Agreement is concluded. For the risk assessment, each Party will use the format set out in [Annex to clause 4.6 Approach A].

Where (A) the one Party chooses not to conduct a risk assessment or will not provide it to the other Party as laid down in the previous paragraph, (B) the other Party has explicitly rejected the provided risk assessment before the Agreement is concluded, or (C) where the risk assessment was not conducted by the one Party in good faith as demonstrated by the other Party, such other Party is only liable for any direct damage caused. This includes, but is not limited to: (i) costs incurred to determine the cause and extent of the damages; (ii) costs 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) [out-of-pocket of other][documented] costs incurred by the aggrieved Party to ensure that its use of the Services is compliant with the Agreement, if the other Party has not cured such breach within the agreed time. Consequential damages such as loss of profit, missed savings or loss of revenue are excluded. Where a series of connected events apply as one event, the one Party's aggregated liability per event towards the other Party for such direct damages as set out in the previous sentence is limited to EUR [*amount].

***Info point 4***

**[Option]**

The Customer may re-assess the risks to reflect changes in the risk situation with regard to the Services at any time. Where the re-assessment results in an increase or decrease of the risk for the Customer, after the second anniversary of the Agreement, each year and to the extent substantiated by the Customer, it may request to negotiate the liability cap for the Services to reflect the change in the risk associated with the Services or additional conditions that should be met, which may include the pricing or amendments to the agreed service-level agreement. If no agreement is reached within [3 months from the Customer’s request] the initially agreed liability cap will remain unchanged, where the Customer then has the right to terminate the part of the Services connected with the increase of risk without any penalties, where the risk cannot reasonably be borne solely by the Customer.

***[Approach B: Limited liability cap: direct damages and maximum amount]***

... is only liable for any direct damage caused. This includes, but is not limited to: (i) costs incurred to determine the cause and extent of the damages; (ii) out-of-pocket or other costs incurred by aggrieved Party 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) out-of-pocket of other [documented] costs incurred by the Customer to ensure that the Services meet the levels of use as agreed in the Agreement, if Provider has not cured such breach within the agreed time. Consequential damages such as loss of profit, missed savings or loss of revenue are excluded. Per event, where a series of connected events apply 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 EUR [*amount].

**[Annex to clause 4.6 Approach A]**

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 amounts are estimated too low, liability for higher damages will be excluded. Where the estimated is 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 | EUR | |
| Data recovery | EUR | |
| Government fines | EUR | |
| Loss of business secrets | EUR | |
| Breach of personal data and remediation actions | EUR | |
| Loss of reputation | EUR | |
| Third-party liability | EUR | |
| **Total risk of potential damages (sum)** | **EUR** | |

***Info point 5***

***Info point 6 on the risk description in the table***

## Info Points - Liability

***Info point 1***: *If the Parties choose to include this Option in their agreement than clause 4.1 should not refer to breaches of confidentiality of Customer's data.*

***Info point 2:*** *The possible optional clause reflects a situation where normally the Providers are not aware of the content of the Customer's data and should not use the Customer's data intentionally for their own purposes. The intention of this option is to guarantee the confidentiality of all Customer data in accordance with the confidentiality obligations – and rights – if and to the extent agreed in the Agreement. On the latter rights, as per applicable law (such as for instance GDPR, NIS2 or the like), a recipient of confidential information may have certain obligations to disclose certain information to certain persons respectively organisations). In contrast, clause 4.2 reflects a situation where the parties agree that the Provider may use some Customer data for pre-agreed and explicitly described purposes.*

***Info point 3***: *See Article 31(2) of the Data Act and Explanatory Note 3: Non-production environment of this SCC.*

***Info point 4:*** *Some examples of how to limit the Party's liability in the event of a series of connected events considered as one event are included in Explanatory Note 5 on Approach A*

***Info point 5:*** *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 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 Customer and Provider or for Customer's specific line of business. You are free to modify it accordingly.*

***Info point 6 on the risk description in the table***:

- *Business interruption: Loss of turnover caused by a breach of contract. You can consider a potential service downtime and its implications on your business or operations.*
- *Data recovery: Assumed costs for recovery of lost, unavailable or corrupted data. Keep in mind that you can be required to implement measures to mitigate your risks, e.g. by having backup data at another provider or on premise.*
- *Government fines against your business are, for instance, fines for violation of data protection laws or regulatory provisions resulting from the provider's operation of the service. Business secrets are protected under law. Disclosure of business secrets can result in loss of business opportunities for your business. Such damages may be recoverable by law.*
- *Loss of business secrets: their disclosure can result in loss of business opportunities. Such damages may be recoverable by law.*
- *You can consider what the impact on your company's reputation will be and what measures will be necessary (e.g. advertising and campaigning to compensate the reputational impact). Such costs may be difficult to recover fully in court proceedings.*
- *Third-party liability covers your potential liability, for instance towards suppliers, customers, subcontractors and third parties.*

**Standard Contractual Clauses (SCCs)**
**For Data Processing Services**
including without limitation: cloud computing services

**SCCs Non-Amendment**

**Explanatory notes for users of the SCCs on Non-Amendment**

**Background**

The Data Act requires providers of data processing services to remove contractual obstacles that might prevent or dissuade a Customer from switching to a new Provider or to an ICT premises. It is important that the parties can rely on the rights and obligations they agreed to contractually and that these rights and obligations are not changed unilaterally, unless otherwise agreed. This is especially true for small and mid-size companies or other organisations, which may not have sufficient resources to assess the possible impact of these unilateral changes on their activities and mission. By considering the inclusion of these standard contractual clauses (SCCs) in their agreement, a Customer may feel more confident when faced with unilateral changes proposed by the Provider. As these standard contractual clauses address relevant scenarios and possible contractual arrangements associated with them, using these SCCs can help ensure such unilateral changes are never detrimental to the interests of either party.

**Explanatory notes**

As a general rule, **the Agreement (including the SCCs) cannot be unilaterally amended** by either party in any way. Only under strict conditions as provided in these SCCs are certain specific unilateral amendments exceptionally allowed.

This is to avoid possible loopholes or unjustified unilateral changes of the agreement. This is reflected in Clauses 1.1 and 1.2 of these SCCs.

These SCCs acknowledge that in certain circumstances the Provider should be able to propose unilateral changes. These are called **Permitted Unilateral Change(s)** and are set out in Clauses 1.2 and 1.5 of these SCCs. A **Permitted Unilateral Change(s)** can only be proposed once and should meet the following conditions:

1. They do not cause any material (contractual, financial, organisational, operational, service-level, legal compliance or other) detrimental effect for the Customer and their use of the Services; and

2. They are notified to the Customer as soon as possible (and in any case, as a rule, no later than 30 days) before to any such proposed **Permitted Unilateral Change(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.

**Standard Contractual Clauses on Non-Amendment**

## I. Definitions

The key terms in these SCCs starting with capital letter are defined in SCC General, Annex 'Definitions'.

## II. Amendment

1.1. Any amendment, revision, update, improvement, supplement or other change to the Agreement (collectively 'Change') must be made in writing and will be subject to the explicit prior mutual consent, including adequate electronic means that guarantee integrity and non-repudiation of the authorised representative(s) of both the Provider and the Customer, except if and to the extent as explicitly provided in Clause 1.2.

1.2. The Provider is only entitled to propose a unilateral Change to the Services, provided that:

A. such Change is clearly beneficial for the Customer, either (A) consists of material enhancement updates of the Services, and/or (B) is necessary for demonstrated security reasons, and/or (C) is required to comply with mandatory applicable law not already in force before the effective date of the Agreement, where items A and B (i) do not breach mandatory law applicable to Customer, and (ii) do not degrade (or other negatively impact the quality or service level of) the Services and the use thereof by Customer, and;

B. all the conditions set out in Clauses 1.3 through 1.5 below ('Permitted Unilateral Change') have been met.

1.3. No proposed Unilateral Change under Clause 1.2 may ever be used by the Provider to directly or indirectly enforce retroactive changes, or to change 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 changing the Agreement;

c. term and termination;

d. liability;

e. representations and warranties, including those set as or in service level(s);

f. confidentiality;

g. methods for the use of subcontracting and methods for the change of subcontractors;

h. access and information rights;

i. qualitative service level objectives;

***Info point 1***

j. Pricing rules or other financial rules;

***Info point 2***

k. the location where the data are processed, if the change would result in data processing or storage outside the EU;

1.4. In the event of a proposed Permitted Unilateral Change, the Provider must:

A. notify the Customer as soon as possible (and in any case no later than 30 days) before any such proposed Permitted Unilateral Change takes effect for the Customer (see 'Permitted Unilateral Change Effective Date'), to allow sufficient time to assess such information and

the internal impact and other potential feasibility and impact it will have or may have for the Customer and their stakeholders, systems and services;

B. provide the Customer, in a complete, correct, and accurate manner, with sufficient and easy-to-understand information and related primary sources of such information, including:

i. the scope, details and timelines of the proposed Permitted Unilateral Change;

ii. why the proposed Permitted Unilateral Change is required;

iii. what the clear benefits are for both Customer and Provider;

iv. what the outcome of the Provider's impact assessment and explanation is of the impact between (a) the prevailing situation and (b) the situation proposed by the Provider after the proposed Permitted Unilateral Change. This must include, without limitation, the short-term, mid-term and long-term contractual, financial, organisational, operational, service-level and legal compliance-related consequences for the Customer, if any. It must also explain why such a Change is clearly beneficial to the Customer as per Clause 1.2.

***Info point 3***

v. the envisaged timeline for deployment and implementation, and the related effective date of the proposed Permitted Unilateral Change entering into force (the 'Permitted Unilateral Change Effective Date').

C. confirm and demonstrate to the Customer that the proposed Permitted Unilateral Change is not in breach of Clauses 1.2, 1.3 and 1.4.

The mandatory notifications and provisions of information set out under this Clause 1.4 must be made in writing and by adequate electronic means.

1.5. Notwithstanding Clause 1.6, if the Provider is able to demonstrate it has complied with Clause 1.4 and the Customer has not explicitly rejected the Permitted Unilateral Change in writing (including without limitation by adequate electronic means) in a substantiated manner before the Permitted Unilateral Change Effective Date, the Customer will be deemed to have accepted the proposed Permitted Unilateral Change at said Permitted Unilateral Change Effective Date. In case the Customer rejects such Permitted Unilateral Change as set forth in the previous sentence, Parties will discuss and aim to settle the matter at hand in good faith, in line with Article 27 Data Act.

1.6. If the provider breaches Clauses 1.1 through 1.5, the Customer will have the right to either obtain from the Provider the Services' restoration to a state prior to the changes, unless duly justified technical unfeasibility by the Provider, or to terminate the Agreement, and at no additional cost. This does not affect the Customer's other rights and remedies, including without limitation the right to seek injunctive relief in any applicable competent court to order Provider to remain providing the Services as agreed, and the right to obtain compensation for the damage suffered (if any).

## Info Points – Non-Amendment

***Info point 1****: Changes regarding already agreed upon 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 Change as per clause 1.2.*

***Info point*** *2: Changes in agreed fees and other financial arrangements including price indexation, other than the underlying rules such as for instance the price indexation methodology itself, may be proposed as a Permitted Unilateral Change as per Clause 1.2.*

***Info point 3***: *clause 1.4 B(iv) refers to the detailed explanation of, and information on, the notified Unilateral Changes and to the general implications for the Customer. Such assessment should address the expected impact with respect to the relevant types of existing customers, taking into account the categories indicated under clause 1.4(B)(iv). This is to ensure that the most likely implications of such a notified Unilateral Change are visible to and understood by the Customer. In this respect, no assessment tailored to individual Customers is provided for under this clause.*