Model Contractual Terms

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

These model contractual terms ('MCTs') are meant to address data access and use and related contractual matters that may arise between a data holder and users (as defined by the Data Act).

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

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

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

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

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

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

1. Parties and Product/Related Service(s)

1.1 Parties to the contract

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

between

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

According to the Data Act, 'data 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 3.2. Based on the contract with the User and on contracts with these third parties, the Data Holder can coordinate data access and use.

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

and

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

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

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

According to the Data Act, '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 MCTs 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 comply with the rules of applicable general contract law and consumer law, according to which terms and conditions may become part of the contract.

1.2 Product/Related Service(s)

This contract is made with regard to:

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

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

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

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

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

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

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

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

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

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

3. Data use and sharing by the Data Holder

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

3.1.1 The Data Holder undertakes to use the Data that are non-personal Data only for the purposes agreed with the User as follows:

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

(b) providing support, warranty, guarantee or similar activities 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 by the Data Holder, by third parties acting on behalf of the Data Holder (i.e. where the Data Holder decides which tasks will be entrusted to such parties and benefits therefrom), in collaboration with other parties or through special purpose companies (such as joint ventures);

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

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

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

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

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

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

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

3.1.2 The Data Holder undertakes not to use the Data:

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

[OPTION] [(b) *(specify data uses that 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 use of the data for particular purposes.

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

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

3.2.1 The Data Holder may share with third parties the Data 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 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 protection measures required under clause 3.4.1; and

iv) [OPTION 1] [not to share these Data further unless the User grants general or specific agreement for such further transferThe Data Holder must oblige the third

party with whom they share Data to include the clauses corresponding to points (i) to (iv) in their contracts with recipients.] [OPTION 2] [not to share these Data further except as set forth in **Appendix 5**.]

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

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

3.3 Use and Sharing of Personal Data by the Data Holder

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

3.4 Protection measures taken by the Data Holder

3.4.1 The Data Holder undertakes to apply the protection measures to prevent Data loss and unauthorised access to the Data [OPTION 1] [that are reasonable in the circumstances, considering the state of science and technology, potential harm suffered by the User and the costs associated with the protective measures.] [OPTION 2] [that are set out in detail in **Appendix 6**.]

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

4. <u>(if applicable) Data access by the User upon request</u>

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

4.1 Obligation to make data available

4.1.1 The Data, together with the relevant metadata necessary to interpret and use those Data must be made accessible to the User by the Data Holder, at the request of the User or a party acting on their behalf. The request can be made using the form specified in **Appendix 2**, sent to (*describe modalities for a simple request through electronic means where technically feasible*).

For the purpose of verifying that the request is made by the User, the Data Holder shall not require to provide any information beyond what is necessary. *(if applicable)* [If the request is made by a party acting on behalf of the User, evidence of their mandate is attached to the request.]

> 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 When the User is not the data subject, the Data Holder shall make the Data which is personal data only available to the User, when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (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.

> 'Metadata' means a structured description of the content or the use of data facilitating the finding or use of those data. According to Article 4 (1), the metadata must be made available with the Data, to the extent that the metadata is "*necessary to interpret and use"* the Data.
>
> Though the relevant metadata needed to interpret and use those data are not laid down and must therefore be identified on a case-by-case basis, the Data Act specifies that "*the data to be made available should include the relevant metadata, including its basic context and timestamp, to make the data 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).

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 and such services may be offered by a provider considered as a gatekeeper under article 3 of Regulation (EU) 2022/1925, unless they process the Data for its own business purposes.

4.2.2 The User must receive access to the requested Data:

(a) easily and securely;

(b) without undue delay;

(if applicable) [(c) continuously and in real-time, if the User requests such access;]

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

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

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

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

- full transfer of the Data, i.e. a copy of the Data is transferred to a medium within the User's control:
- by way of transmission triggered by the Data Holder (push), such as online transmission, upload into the User's cloud space or delivery of a tangible medium on which the Data is stored; or
- by way of retrieval triggered by the User (pull), such as on being provided with an API, access to the Data Holder's cloud space or similar tools that enable the User to access and extract the Data; or
- access to the Data where 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 User 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 User's control, unless special arrangements are taken.

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

However, full transfer significantly reduces the Data Holder's ability to prevent abuse and to protect their interests, e.g. trade secrets. Therefore, access and processing where the Data is stored should also be possible. To reconcile such access with the interests of the User, 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.

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

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

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

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

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

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

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

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

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

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

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

4.3 Feedback loops

If the User identifies an incident related to clause 2 on the Data covered by the Contract, to the requirements of clauses 4.2.1 or 4.2.2 or of **Appendix 1** on the Data characteristics and access arrangements and if the User 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 within a reasonable period of time. If the Data Holder does not do so, it is considered as a fundamental non-performance and the User may invoke clause 12 of this contract). If the User considers their access right under Article 4 (1) of the Data Act to be infringed, the User is also entitled to lodge a complaint with the competent authority, designated in accordance with Article 37(5), 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 non-performance 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 unilaterally change the specifications of the Data characteristics or the access arrangements stated in **Appendix 1**, if this is objectively justified by the normal conduct of business of the Data Holder, for example by a technical modification due to an immediate

security vulnerability in the line of the products or related services or a change in the Data Holder's infrastructure. Any change must meet the requirements of clauses 4.2.1 and 4.2.2.

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

A shorter notice period may suffice:

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

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

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.

   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.

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

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

   Data can only be 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 4 of the Data Act.

   See clause 5.1.1.

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

   See clause 5.1.2.

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

   See clause 5.1.3.

4. **Audit rights -** In order to preserve the confidentiality of the Data protected as trade secrets, while not interfering with each 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.

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

   See clauses 5.2 and 5.3.

6. **Trade secret holder rights (2/4)** – If the initial measures do not suffice, the trade 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 5.4.1.

7. **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 5.4.2.

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

   See clause 5.4.3.

9. **Retention of Data containing Identified Trade Secrets** – If the Data Holder withholds or suspends data sharing in accordance with clauses 5.4.1, 5.4.2 or 5.4.3, the Data Holder will still be obliged to keep the related Data containing Identified Trade Secret readily available by retaining it up to the moment that it can be shared within scope of the Contract.

   See clause 5.6.

10. **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 5.1.2.

5.1 Applicability of trade secret arrangements

5.1.1 The protective measures agreed on in clauses 5.2. and 5.3 of this contract, as well as the related rights agreed in 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 and the identity of the Trade Secret Holder(s) are set out in **Appendix 4**.

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

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

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

5.1.3 If, during this contract, new data are made available to the User that 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 **Appendix 4** has been amended and agreed between the Parties, the Data Holder may temporarily suspend the sharing of the new data protected as trade secrets. In such case, the Data Holder must give notice to the User and the competent authority designated under Article 37 of the Data Act. The notice must be duly substantiated, indicate which measures have not been agreed, and be given in writing without undue delay.

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

5.2 Protective measures taken by the User

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

Parties should, in a separate appendix, 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 (i) access is to be provided where the Data are stored or (ii) the Data are to be fully transferred to the user. In the former case, the Data Holder has a higher degree of control and can apply part of the protective measures 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.

5.2.2 If the User is permitted to make Data protected as trade secrets available to a third party, the User must inform the Data Holder without undue delay of the fact that Data protected as 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, place of establishment 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 User's Protection 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 clauses 5 and **Appendix 4** as applicable at that time. The results of the audit reports will be submitted to both Parties without undue delay.

The User may choose between (i) and (ii). If a Party deems the security audit report obtained at the other party's expense is not correct, they retain the right to obtain security audit report from another independent third party at their own expense. 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 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 User's Protection Measures.

5.3 Protective measures taken by the Trade Secret Holder

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

5.3.2 The Data Holder may 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 the Data Holder's protection measures nor the measures taken in accordance with clause 5.3.2, unless otherwise agreed by the Parties.

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

5.4.1 Where the Identified User's Protection Measures and the Data Holder's Protection Measures do not materially suffice to adequately protect a particular Data protected as 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 their 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 Data in question. In such case, the Data Holder must give notice to the User. The notice must be duly substantiated, indicate which measures have not been agreed, and be given in writing without undue delay. The Data Holder must continue to share any Data protected as trade secrets other than these specific Data.

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

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

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

Refusal or discontinuation of data sharing under Article 4 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 trade secret in question or the uniqueness and novelty of the relevant connected product.

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

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

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

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

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

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

(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 the Data Holder exercises the right to refuse, withhold or suspend the data sharing to the User in accordance with clauses 5.4.1, 5.4.2 and 5.4.3, 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 to the extent the withholding or suspension of Data sharing occurs in accordance with 5.4.3**.**

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

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

6.2 Unauthorised use and sharing of data and restrictions for security reasons

6.2.1 The User undertakes not to engage in the following:

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

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

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

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

6.2.2 [OPTION] [Furthermore and in accordance with article 4 (2) of the Data Act, the User and the Data Holder agree to restrict or prohibit as follows the following processing (*specify concerned processing: access, use and/or further sharing of Data*), having as a consequence to undermine security requirements for the Product, as laid down by EU law (*specify concerned legal security requirement*) resulting in a serious effect on the health, safety or security of natural persons.

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

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

7.1 Making Data available to a Data Recipient

7.1.1 The Data, together with the relevant metadata necessary to interpret and use those Data, must be made available to a Data Recipient by the Data Holder, free of charge for the User, upon request presented by the User or a party acting on 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*). For the purpose of verifying that the request is made by the User, the Data Holder shall not require to provide any information beyond what is necessary.

7.1.2 When the User is not the data subject, the Data Holder shall make the Data which is personal data only available to a third party following a request of the User, when there is a valid legal basis for making personal data available under Article 6 of Regulation (EU) 2016/679 (GDPR) and only, 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 in accordance with Chapter III and Chapter IV of the Data Act.

7.1.5 The User acknowledges that a request under clause 7.1.1 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].

7.1.6 The User acknowledges that the third party shall only process the Data made available to them pursuant to clause 7.1.1 for the purposes and under the conditions agreed with the User. The Data Holder may not be held liable towards the User for the absence of such an agreement between the User and the third party, unless the Data Holder knew or should have known about this absence.

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

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

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

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

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

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

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

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

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

9. Compensation to the User

9.1 Compensation

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

The Parties can agree on 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 8, the User should be compensated, as explained in the explanatory box under clause 8, and the compensation should be proportionate to the value of the limitation,

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

If a compensation is due, the parties must agree on its nature, that can be monetary or not.

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

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

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

Right of the Data Holder to use the Data

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

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

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

In other situations, it may still be feasible and preferrable that the initial User notifies the Data Holder of the contact details of an additional User, in such a manner that the Data Holder can concludes a contract directly with the latter.

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

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

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

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

- User's Removable Data – the products or related services often allow the user to delete the Data generated in the course of their use. In the case of transfer, the user should delete such Data. Otherwise, such Data may be accessible to the additional or subsequent user;

- Always Removable Data – Data which the Data Holder should not make accessible to the additional or subsequent user;
- Residual Data – 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 additional or subsequent user by operation of law or in practice (for example, related to the updates made in a connected vehicle).

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

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

10.1 Transfer of use

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

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

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

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

10.2 Multiple users

Where the initial User grants a right to use 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.

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

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

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

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

10.2.2 Data Access by the Additional User

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

10.3 Liability of the Initial User

To the extent that the initial User's failure to comply with their obligations under clauses 10.1 and 10.2 leads to the use and sharing of Product or Related Services Data by the Data Holder in the absence of a contract with the Subsequent or Additional User, the initial User will indemnify the Data Holder in respect of any claims for damages by the Subsequent or Additional User towards the Data Holder for their use of the Data after the transfer or temporary use of the Product and/or Related Service(s).

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

11.1 Date of application and duration

> This set of MCTs would usually not exist as a standalone contract, but be concluded in parallel with the contract transferring ownership of the Product to the User, giving him temporary rights to use the Product and/or with the contract for a Related Service.
>
> This Contract must generally remain into force as long as this other contract allows the User to use the Product or Related Service. Similarly, neither the Data Holder nor the User should be able to terminate this Contract except where there is a substantive breach of obligations by the other Party, as this would otherwise result in a situation in which the User uses the Product and/or Related Service without any contractual framework regarding rights and obligations under the Data Act.

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

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

11.2 Termination

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

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

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

(c) when both Parties so agree.

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

11.3 Effects of expiry and termination

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

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

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

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

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

12. Remedies for breach of contract

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

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

12.1 Cases of non-performance

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

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

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

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

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

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

12.2 Remedies

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

12.2.2 Remedies which are not incompatible may be cumulated.

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

12.2.4 The aggrieved Party can:

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

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

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

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

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

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

12.2.6 The User can also:

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

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

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

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

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

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

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

13. General Provision

13.1 Confidentiality

13.1.1 The following information will be considered as confidential:

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

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

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

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

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

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

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

13.1.4 These confidentiality obligations do not remove any more stringent obligations under (i) the Regulation (EU) 2016/679 (GDPR), (ii) the provisions implementing Directive 2002/58/EC or

Directive (EU) 2016/943, or (iii) any other EU or Member State law (iv) (if applicable) clause 6 of this Contract.

13.2 Means of communication

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

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

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

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

13.3 Entire Contract, modifications and severability

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

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

13.3.3 If any provision of this Contract is found to be void, invalid, voidable or unenforceable for whatever reason, and if this provision is severable from the remaining terms of the contract, these remaining provisions will continue to be valid and enforceable. Any resulting gaps or ambiguities in this Contract shall be dealt with according to clause 13.5.

13.4 Applicable law

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

13.5 Interpretation

13.5.1 This Contract is concluded by the Parties against the background of the Parties' rights and obligations under the Data Act. Any provision in this Contract must be interpreted so as to comply with the Data Act and other 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 must be interpreted in the light of the rules of interpretation provided for by the applicable law (see clause 13.4).

13.6 Dispute settlement

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

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

13.6.3 [OPTION, if the user is a business] [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 the content of the data

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

B. Duration of retention

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

C. Data regime

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

D. Data structure and format

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

E. Access policy

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

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

needs to be accessible to the Subsequent User by operation of law or in practice (for example, related to the updates made in the connected vehicle

F. Transfer/Access Medium

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

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

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

Appendix 2: 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).

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

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

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

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

This form is for one particular request. Multiple requests are possible under 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* Contract n°: *Specify*
Identification of the person making the request on behalf of the User (if applicable)	Name: *Specify* Relationship with the User: *Specify*
Products and/or Services concerned by the request	Product/Service 1: *Specify* Product/Service 2: *Specify*
Data concerned by the request **Please note:** does not apply in the context of the testing of new connected products, substances or processes that are not yet placed on the market	☐ Option 1: All data which is readily available to the Data Holder ☐ Option 2: *Specify, in accordance with Appendix 1 of the contract between the User and the Data Recipient specifying the Data to be shared with the Data Recipient* ☐ Option 3: As specified by the Data Recipient in appendix 2 of the contract between the Data Holder and the Data Recipient
If the data includes personal data	*Specify valid legal basis for processing under Article 6 of Regulation (EU) 2016/679 and, where relevant, how the conditions of Article 9 of that Regulation and of Article 5(3) of Directive 2002/58/EC are fulfilled*
Identification of the third party **Please note:** cannot be a gatekeeper under Article 3 of Regulation (EU) 2022/1925	Name: *Specify* 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)

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

(to be drafted by the parties)