Model Contractual Terms under the Data Act.

Trackunit is committed to providing our customers and partners the best level of security within our industry. To that effect Trackunit only processes data on the right legal basis, this includes any transfer and processing of data outside the EU. Trackunit upholds the principles of the General Data Protection Regulations and the Data Act, and any transfer of processing of data based on the Model Clause Terms as set out below. Depending on the role of you as a Customer of Trackunit, several modules may apply.
You may have several roles where you are both a Data Holder, Data User and/or Data Recipient in which case several Annexes respectively will apply to the processing of data between you and Trackunit.

In any instance where Trackunit is acting as a processor on behalf of you as a Customer, you are responsible for creating the correct contractual framework with your customers. Trackunit will act on your instructions, as a processor. The below Annexes are only intended to create a framework between you and Trackunit in which you are a direct Customer of Trackunit. If Trackunit is acting as Data Holder on behalf of third party, you as a Data User or a Data Recipient are responsible for creating the correct contractual framework with the main Data Holder.

In the event that you as a Customer need to switch data provider, as described in the Data Act. The provisions in the Standard Contractual Clauses as presented below shall apply.

General provisions shall apply for all Annexes as described in Annex I Section 12.

ANNEX I. MODEL CONTRACTUAL TERMS

for contracts on data access and use between data holders and users of connected products and related services

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

Trackunit and/or Customer ('Data Holder')

and

Customer and/or Trackunit ('User')

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

1.2 Product/Related Service

This contract is made with regard to:

(a) **the following connected product(s) (the 'Product'):** ***Telematics services and hardware as described on Trackunit website)*****;**

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.

The User commits to provide upon duly substantiated request to the Data Holder any relevant

documentation to support these declarations, where necessary.

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 A**, 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 A** will be amended accordingly.

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.**

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;**

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 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;**

(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**

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). Parties agree to always uphold and treat Personal Data and privacy in general in the manner as stated on Trackunit website, as it relates to data being shared between the Parties.

3.4 Protection measures taken by the Data Holder

3.4.1 **The Data Holder undertakes to apply the protective measures for the Data 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.**

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

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.**

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 A,** the Raw Data collected by Trackunit Hardware is listed in Appendix A to these Agreements.

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 by the Data being transmitted and/or by access to the Data where it is stored;**

The Data Holder must specify these access arrangements and inform the User of these specifications in **Appendix A,** the Raw Data collected by Trackunit Hardware is listed in Appendix A to these Agreements.

.

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 A**, which forms an integral part of this Contract.

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 A** 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 within a reasonable period of time. 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.

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 A**, 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 within 14 days 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 30 days 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

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) shall be provided by Customer to Trackunit and will form 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.**

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, the Identified Trade Secrets will be amended accordingly.**

Until the Trade Secret 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

5.2.1 **The User must apply the protective measures (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.**

5.3 Protective measures taken by the Data Holder

5.3.1 **The Data Holder may apply any appropriate technical and organisational protection measures 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.

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.

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 30 days, 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.

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.**

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 Compensation to the User

8.1 Compensation

The Data Holder undertakes to compensate the User as set out in the overall contractual agreement between the Parties, which forms an integral part of this Contract.

9 Transfer of use and multiple users

9.1 Transfer of use

9.1.1 **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.**

9.1.2 **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.**

9.1.3 **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.**

9.2 Multiple users

9.2.1 **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.**

9.2.2 **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.

9.3 Liability of the Initial User

If the User's failure to comply with their obligations under clauses 9.1 or 9.2 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.

10 Date of application and duration of the Contract and Termination

10.1 Date of application and duration

10.1.1 **This Contract takes immediate effect when the Customer has agreed to Trackunit standard Terms and Condition.**

10.2 Termination

Irrespective of the contract period agreed under clause 10.1, 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.

10.3 Effects of expiry and termination

10.3.1 **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 12.1 on confidentiality, clause 12.3 on applicable law and clause 12.6 on dispute resolution, which remain in full force and effect.

10.3.2 **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.

11 Remedies for breach of contract

11.1 Cases of non-performance

11.1.1 **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.

11.1.2 **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.

11.2 Remedies

11.2.1 **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.**

11.2.2 **Remedies which are not incompatible may be cumulated.**

11.2.3 **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.**

11.2.4 **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 11.1.2. 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.

11.2.5 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;

11.2.6 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 General Provision

12.1 Confidentiality

12.1.1 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;

12.1.2 **Both Parties agree to take all reasonable measures to store securely and keep in full confidence the information referred to in clause 12.1.1. 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.

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

12.1.4 **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.**

12.2 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 respective business addresses:
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.**

12.3 Applicable law

This Contract is governed by the law of Denmark).

12.4 Entire Contract, modifications and severability

12.4.1 **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.**

12.4.2 **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.**

12.4.3 **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 12.5.

12.5 Interpretation

12.5.1 **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.**

12.5.2 **If any gap or ambiguity in this Contract cannot be resolved in the way referred to by clause 12.5.1, 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.**

12.6 Dispute settlement

12.6.1 **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).

12.6.2 **Submission of a dispute to a dispute settlement body in accordance with clause 12.6.1. 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.**

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

Customer or Trackunit ('User') and
Trackunit or Customer ('Data Recipient') hereinafter referred to collectively as 'the Parties' and individually as 'the Party'.

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, the User will request the Data Holder to make the Data specified in clause 2 available to the Data Recipient or the User mandates the Data Recipient to request the 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').**

1.2.3 **The request should be made and the H2R Contract should be concluded agreed between all Parties. If the request concluded 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'):** ***Telematics services and hardware as described on Trackunit website)***

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.

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

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 within the meaning of the Data Act and as listed in **Appendix A**.

The User expressly disclaims and waives all warranties regarding quality, characteristics and quantity of the Data and its fitness for a particular purpose.

3. Data use by the Data Recipient

3.1 Authorised use of the Data

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

3.1.1 **The Data Recipient must erase or fully anonymize 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;**

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).

3.4 Application of protective measures

The Data Recipient undertakes to apply protective measures for the Data 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.

4. Data sharing with third parties and data processing services

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 agreed between the Parties 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; 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 agreed, it should in a detailed manner notify the User in accordance with notification rules. 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.

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 Data Recipient undertakes to compensate the User as set out in the overall contractual framework between the Parties**,** 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

7.1 Duration and termination

7.1.1 **This Contract comes into effect when Customer has agreed to Trackunit Terms and Conditions 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 as specified in Trackunit Terms and Conditions to the User if the H2R Contract has been terminated.**

7.1.3 **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**

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 direct 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 direct loss suffered by the aggrieved Party. This amount shall not exceed the standard limitation of liability stated in Trackunit standard Terms and Conditions.

(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.**

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

Customer or Trackunit ('Data Holder') and

Trackunit or Customer ('Data Recipient')

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

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 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:** ***Telematics services and hardware as described on Trackunit website.***

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 A.**

2.1.3 **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.

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 the purposes listed in Section 1.2 to this Annex III.**

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.**

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.**

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 A, which forms an integral part of this Contract.**

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 by the data being transmitted orby access to the Data where it is stored;

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 A, 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.

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 within a reasonable period of time. 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 within 14 days 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 30 days 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

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 in an agreement between the Parties, 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. 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, the agreement will be amended accordingly.

Until the Trade Secret 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.

4.1.3 **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 in the overall contractual framework between the Parties (hereafter these are referred to as '*Identified Trade Secrets DR Measures*').**

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.**

4.3 Protective measures taken by the Data Holder

4.3.1 **The Data Holder may apply the measures set out in detail in the overall contractual framework 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.

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 30 days, 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.**

6.1.2 **The Parties agree that the Data Recipient will compensate the Data Holder as defined in the overall contractual framework between the Parties.**

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.**

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 as agreed in the overall contractual framework between the Parties.**

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.**

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 comes into effect when Customer has agreed to Trackunit standard Terms and conditions and are subject to any grounds for expiry or termination under this Contract.**

7.1.2 **The Data Holder must start making the Data available to the Data Recipient without undue delay after the Contract has come into effect.**

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 as agreed between the Parties or as indicated in Trackunit standard Terms and Conditions. The Data Recipient must notify the Requesting User that the Contract has been terminated.**

Where the Data Recipient terminates the Contract under this clause before the minimum subscription period, they must compensate the Data Holder for the costs incurred by the Data Holder for making the data available.

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. This may, depending on the circumstances, include such exit support measures as the Data Recipient may reasonably expect.**

8 Remedies for breach of 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.**

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

Customer or Trackunit] ('Data Sharer') and

Trackunit and Customer ('Data Recipient') hereinafter referred to collectively as

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

2. Data covered by the Contract

The data covered by this Contract ('the Data') consists of the Data identified in **Appendix A**, 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 as well as to take appropriate measures to protect such Data in accordance with the applicable regime.

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: Trackunit or Customer systems, or any designated third party hosting the data on behalf of either Trackunit or Customer.**

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 A 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 **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 **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 professional-, ethical industry-, cybersecurity-, research- and AI-standards.**

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 **The overall contractual framework between the Parties shall contain 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.**

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

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.**

The Data Sharer represents that the Data is adapted to the following context of processing by the Data Sharer in accordance with usual expectations.

The Data Sharer represents that the Data is fit for the objectives pursued by the Data Recipient.

Specific quality requirements: The Data Sharer shall make the following available to the Data Recipient, 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.

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

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.**

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; as agreed between the Parties.

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 as agreed between the Parties.

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) **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.**

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, 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 as defined between the Parties when making the data available under one or more options under 4.2.1.**

.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 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 agreed details 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 ***(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 30 days, 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: The Data Recipient may process the Data only for the purposes as agreed between the Parties Authorized Purposes").**

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

The Data Recipient may only implement the following operations on the Data: as agreed between the parties. ("Authorized Operations").

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 for the duration of the Contract.**

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.**

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) **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**
- **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.**

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

6.1 Applicability of trade secret arrangements

6.1.1 **The protective measures as well as the related rights agreed below apply exclusively to data or metadata included in the Data to be 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 B. 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 in the overall contractual framework between the Parties (hereinafter: 'Identified Trade Secrets DR Measures').

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 the overall contractual framework between the Parties 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.

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. The Parties will abide by the IP sections set up in the overall contractual framework between the Parties.**

8. Compensation for provision of data access

The Parties agree that the Data Recipient will compensate the Data Sharer as agreed in the overall contractual framework between the Parties.

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 without undue delay after the Contract has come into effect.

9.2 (if applicable) Duration

This Contract is subject to the overall contractual framework between the Parties and will terminate when the overall contractual framework is concluded.

9.3 Termination for convenience

9.3.1 **The Data Recipient may terminate the Contract in accordance with Trackunit standard Terms and Conditions.**

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.**

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 the limitations of liability as defined in Trackunit standard Terms and Conditions.

(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

Trackunit

Standard Contractual Clauses for Data Act

1. **SCC Agreement**

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

a. **SCC General with Annexes**
b. **SCC Switching & EXIT**
c. **SCC Termination**
d. **SCC Security and Business Continuity**
e. **SCC Non-Dispersion**
f. **SCC Liability**
g. **SCC Non-Amendment**

The aforementioned SCCs separately and collectively form an integral part of the SCC Agreement. Any reference to the SCC Agreement shall be deemed to include a reference to said documents.
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 SCC 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

2. **Definitions**

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

SCC 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 SCC Agreement(s), including without limitation its Annexes;

Annex means an annex, schedule or exhibit explicitly referenced in the SCC Agreement;

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 SCC 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;

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;

Data Act means Regulation (EU) 2023/2854 ('DA');

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;

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 SCC Agreement, the said data processing services regard those provided or to be provided by Provider to Customer as agreed under the SCC Agreement, not being Other Services;

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;

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;

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;

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 SCC Agreement;

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;

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 SCC Agreement;

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 SCC Agreement;

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;

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 SCC Agreement;

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

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;

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

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

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

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

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;

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 SCC Agreement;

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;

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

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 SCC Agreement;

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;

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.

3. **SCC Switching and Exit**

In the event that Customer wishes to Switch to another provider, and wishes to transfer the data as specified in Appendix A Customer can utilize two options.

a. **Option A:**
   Customer wishes assistance of Trackunit to transition the data to themselves or a third party provider;
   i. **Trackunit and Customer will together work out a Switching Plan and applicable fees for such a transition. The Switching Plan will contain fees, deadlines, technical information on receiving system, and further information needed of the transfer. If Customer requires other data transferred than what is explained in Appendix A, this can be negotiated between the Parties, if such a wish is possible.**
   ii. **As per the Data Act, any Switching Plan shall be worked out between the Parties within a 14 day period, after the Customer has provided Trackunit with a Switching Notice. A Transitional Period will be included in the Switching Plan, and cannot exceed 7 months, unless Customer is requesting other Data than provided in Appendix A.**
   iii. **Customer and Trackunit will provide reasonable assistance during the Transitional Period. Customer and Trackunit will take reasonable measures to achieve effective switching.**
   iv. **Customer and any third party designated by Customer will respect any and all intellectual property rights of any material provided by Trackunit during the switching process.**
   v. **Upon a successful switch Customer shall notify Trackunit that the switching process has been successfully completed, and that the Switching Plan has been executed,**

effectively terminating this SCC Agreement.

b. Option B:

Customer wishes self service using Trackunit API.

i. Customer shall notify Trackunit that they wish to switch provider, either to a third party, or undertake the Processing themselves.

ii. Trackunit will make available the Data as specified in Appendix A, via an API.

iii. Customer is responsible for interoperability and data accuracy in the receiving system. Trackunit will only make the API available to Customer, so that the data can be transferred.

iv. Customer shall notify Trackunit when the switch is completed. Customer is obliged to transfer any and all data prior to any subscription with Trackunit expiring. Post expiration all that located in Trackunit systems will be deleted or anonymized per Trackunit standard, as described on Trackunit website.

4. **Termination**

This SCC Agreement will be considered terminated between the Parties, when one of the following events has occurred in full:

i. The switching process has been successfully completed.

ii. Customer has terminated their entire agreement with Trackunit, and all subscriptions has been terminated.

iii. A Party has been declared bankrupt.

iv. A Party is in breach of the obligations of this SCC Agreement, or the overall Trackunit Standard Terms and Conditions.

v. A Party has experience a change in ownership that by law results in a termination of this SCC Agreement.

5. **Security and Business Continuity**

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.

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.

5.1. **Security**

Further to clause 5, 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.

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:

5.1.1. 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

5.1.2. any other risks concerning and otherwise related to effective switching.

5.2. Such measures as laid down in clauses 5.1.1 and 1.2 must – for any service model and any deployment model – at least ensure, without limitation:

5.2.1. ongoing confidentiality, integrity, availability of the data and resilience of the services, exportable data and digital assets;

5.2.2. 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

5.2.3. 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.

5.3. 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.

6. Business Continuity

Further to clause 5.1, the Provider must in particular:

6.1. act with due care to maintain business continuity and continue to provide the services under the agreement;

6.2. provide clear information concerning known risks to continuity in the provision of the services; and

6.3. The Provider must ensure that they notify the Customer as laid down in clause 5, 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.

6.4. 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.

7. Miscellaneous

7.1. At the Customer's request, the Provider must, without undue delay, provide the Customer with a summary of the key elements of the Provider's security measures and related security management, and of its business continuity and related contingency management and of any material changes to any of the above.

7.2. 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.

8. SCC Non-Dispersion

8.1. 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.

8.2. Contractual arrangements must include, without limitation:

8.2.1. 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;

8.2.2. 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;

8.2.3. 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.

9. SCC's Liability

9.1. In cases where the obligations under this SCC 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, willful misconduct or gross negligence, such Party is liable for any and all damages, without limitation. The previous sentence is subject to clause 9.5.

9.2. The Provider is only allowed to use Customer data for purposes explicitly described in the SCC Agreement and any further agreements between the Parties, 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.

9.3. All Customer data processed under the SCC Agreement must be qualified as confidential and are therefore subject to the confidentiality obligations as laid down in the SCC Agreement and overall contractual agreement between the Parties. Except as stated in clause 9.4, in cases where such obligation is breached, the Provider is liable for all damages, without limitation.

9.4. The Provider's unlimited liability as stated in clause 9.3 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.

9.5. The Provider is not liable for

9.5.1. 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 SCC 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

9.5.2. 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.

9.6. Except as otherwise set forth in the clauses 9.1 and 9.5, a 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) 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 the limitation of liability as set out in Trackunit standard Terms and Conditions.

10. **SCCs Non-Amendment**

10.1. **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 10.2.**

10.2. **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 10.3 through 10.5 below ('Permitted Unilateral Change') have been met.**

10.3. **No proposed Unilateral Change under Clause 10.2 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;**
j. **Pricing rules or other financial rules;**
k. **the location where the data are processed, if the change would result in data processing or storage outside the EU**

10.4. **In the event of a proposed Permitted Unilateral Change, the Provider must**

10.4.1. **notify the Customer as soon as possible (and in any case no later than 14 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;

10.4.2. 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:

10.4.2.1. the scope, details and timelines of the proposed Permitted Unilateral Change;

10.4.2.2. why the proposed Permitted Unilateral Change is required;

10.4.2.3. what the clear benefits are for both Customer and Provider;

10.4.2.4. 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 10.2.

10.4.2.5. 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').

10.4.3. confirm and demonstrate to the Customer that the proposed Permitted Unilateral Change is not in breach of Clauses 10.2, 10.3 and 10.4.

10.5. **Notwithstanding Clause 10.6, if the Provider is able to demonstrate it has complied with Clause 10.4 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**

10.6. **If the provider breaches Clauses 10.1 through 10.5, 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).**

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

Trackunit ApS – Data Disclosure Sheet (EU Data Act)

Version: 1.0 | Date: 25 September 2025

This document describes the categories of data collected by Trackunit devices and related services and is intended to support the pre-contractual transparency obligations under the EU Data Act (Regulation (EU) 2023/2854). It complements contract terms, data processing agreements and product documentation.
Important notes:

- **The availability of each data point may depend on installation, configuration, connected sensors, and the customer's selected features.**
- **For Bluetooth tags (Trackunit Kin), data is collected when seen via compatible gateways (e.g., Trackunit Raw or Beam).**
- **Personal data processing (if any) is governed by GDPR roles and the parties' Data Processing Agreement or Standard Contractual Clauses.**

Trackunit Raw

Sensor / Data Point	Description
GPS / Positioning	GPS position (Latitude, Longitude) along with number of satellites, SNR, speed, altitude, direction, HDOP, EHPE
Distance and driving time	The device calculates distance and driving time
3-Axis Accelerometer	Motion / vibration / utilization detection(movement)
3-Axis Gyroscope	Tilt, turnover detection (rotation/orientationchanges)
Temperature Sensor	Measures ambient temperature
Light Sensor	Measures if the device case is opened
Dual CAN-Bus (CAN-FD, auto-baud)	Collects machine telemetry from the machine's CAN network (e.g. engine, hydraulics, fault codes) assuming wiring/connectivity is provided
RS485 / Modbus	Serial connection for additional telemetry via Modbus (if harnessed and configured)
Analog / Digital Inputs	The TU700 has 6 digital/analog input channels; these allow collecting external signals (e.g.ignition status, hour meter, sensors wired in)
Quality of signal(Bluetooth / Cellular / Wifi / GNSS)	The device monitors and reports signals from both short- and long-range wireless technologiesIncluding: COPS, band, RAT, RSSI, Cell ID
Battery / Power Status	The device monitors supply voltage; has internal battery backup/storage.

Machine Utilization	The device measure machine utilization time based on GNSS, Accelerometer, Digital Inputs
Bluetooth	For recognized tags: The position where the tag was seen, The time the tag was seen, the Tags's RSSI , the tags IDs
Debug / Statistic data	The device collects and reports additional data used for debugging and statistical purposes
Hardware info	The device reports external and internal hardware components IDs and firmware versions (e.g.cellular, SIM card)
Access Management	The device reports keypad connection status, equipment lockout status, status/versioning indicating successful upload of user credentials on the device.

Trackunit Spot

Sensor / Data Point	Description
GPS / Positioning	GPS position (Latitude, Longitude) along with number of satellites, SNR, speed, altitude, direction, HDOP, EHPE
3-Axis Accelerometer	Motion / vibration / utilization detection(movement)
3-Axis Gyroscope	Tilt, turnover detection (rotation/orientationchanges)
Temperature Sensor	Measures ambient temperature
Light Sensor	Measures if the device case is opened
Quality of signal(Bluetooth / Cellular / Wifi / GNSS)	The device monitors and reports signals from both short- and long-range wireless technologiesIncluding: COPS, band, RAT, RSSI, Cell ID
Battery / Power Status	The device monitors supply voltage; has internal battery backup/storage.
Machine Utilization	The device measure machine utilization time based on GNSS, Accelerometer, Digital Inputs
Debug / Statistic data	The device collects and reports additional data used for debugging and statistical purposes
Hardware info	The device reports external and internal hardware components IDs and firmware versions (e.g.cellular, SIM card)

Trackunit Beam

Sensor / Data Point	Description
GPS / Positioning	GPS position (Latitude, Longitude) along with number of satellites, SNR, speed, altitude, direction, HDOP, EHPE
3-Axis Accelerometer	Motion / vibration / utilization detection(movement)

3-Axis Gyroscope	Tilt, turnover detection (rotation/orientationchanges)
Temperature Sensor	Measures ambient temperature
Light Sensor	Measures if the device case is opened
Analog / Digital Inputs	The TU700 has 6 digital/analog input channels; these allow collecting external signals (e.g.ignition status, hour meter, sensors wired in)
Quality of signal(Bluetooth / Cellular / Wifi / GNSS)	The device monitors and reports signals from both short- and long-range wireless technologiesIncluding: COPS, band, RAT, RSSI, Cell ID
Battery / Power Status	The device monitors supply voltage; has internal battery backup/storage.
Bluetooth	For recognized tags: The position where the tag was seen, The time the tag was seen, the Tags's RSSI , the tags IDs
Debug / Statistic data	The device collects and reports additional data used for debugging and statistical purposes
Hardware info	The device reports external and internal hardware components IDs and firmware versions (e.g.cellular, SIM card)

Trackunit Kin (via gateway)

Sensor / Data Point	Description
Temperature Sensor	Measures ambient temperature
Operation time	Counters with information about total amount of time spend in specific modes and time since last activity
Utilization	Accumulated Asset Activity, moving time in seconds
Battery level	Own battery level
Accelerometer	Number of seconds since last G-force event and G-Force value
Tx power	RF power used to transmit data

EU Data Act – User Access & Sharing Rights (Summary)

- **Access: Data Users of connected products may access data generated by their use (raw and certain pre-processed data) in a structured, commonly used, machine-readable format, within the parameters agreed with the Data Holder.**
- **Sharing: Data Users may instruct Trackunit to share their data with authorized third parties. Sharing is subject to security and lawful basis requirements.**
- **Transparency: Before entering a contract, Data Users are informed of the types of data generated, frequency/volume, how to access/share it, and relevant limitations.**
- **Use Limitations: Non-personal data originating from the Data User shall not be used to compete with the Data User's product and requires consent for provider reuse beyond service delivery.**

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

(to be drafted by the parties)