Annex 1 – Customer Data Protection Provisions

A. DEFINITIONS AND INTERPRETATION

A.1 Definitions

"**Appropriate Safeguards**" means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

"**Data Processing Losses**" means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation to a Data Subject ordered by a Supervisory Authority; and

(iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

"**Data Protection Laws**" means as applicable and binding on the Customer, Supplier or the Services:

(a) in the UK:

(i) the Data Protection Act 1998 ("**DPA 1998**") and any laws or regulations implementing Council Directive 95/46/EC ("**Data Protection Directive**"); and/or

(ii) the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"), and/or any corresponding or equivalent national laws or regulations ("**Revised UK DP Law**");

(b) in other EU countries: the Data Protection Directive or the GDPR, once applicable, and all relevant Member State laws or regulations giving effect to or corresponding with them;

"**Data Subject Request**" means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

"**Complaint**" means a complaint or request relating to either party's obligations under Data Protection Laws relevant to this agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

"**DPIA**" means a data protection impact assessment, in accordance with Data Protection Laws;

"**GDPR Date**" means from when the GDPR applies on 25 May 2018;

"**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

"**Protected Data**" means Personal Data received from or on behalf of the Customer in connection with the performance of Supplier 's obligations under this agreement;

"**Sub-Processor**" means another Data Processor engaged by Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Customer;

"**Supervisory Authority**" means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

A.2 Interpretation

In this agreement:

A.2.1 "**Data Controller**" (or "controller"), "**Data Processor**" (or "processor"), "**Data Subject**", "**international organisation**", "**Personal Data**" and "**processing**" all have the meanings given to those terms in Data Protection Laws (and related terms such as "**process**" have corresponding meanings);

A.2.2 references to the DPA 1998 or the Data Protection Directive and to terms defined in that Act or in that Directive shall be replaced with or incorporate (as the case may be) references to any laws replacing, amending, extending, re-enacting or consolidating such Act or Directive (including the GDPR and the Revised UK DP Law) and the equivalent terms defined in such laws, once in force and applicable; and

A.2.3 to the extent that a term of this agreement requires the performance by a party of an obligation "in accordance with Data Protection Laws" (or similar), unless otherwise expressly agreed in this agreement, this requires performance in accordance with the relevant requirements of such Data Protection Laws as are in force and applicable at the time of performance (if any).

1. DATA PROTECTION

1.1 **Processor/Controller**

1.1.1 The parties agree that, for the Protected Data, the Customer shall be the Data Controller and Supplier shall be the Data Processor.

1.2 **Compliance with Data Protection Laws and obligations**

1.2.1 Supplier shall process Protected Data in compliance with:

(a) the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this agreement; and

(b) the terms of this agreement.

1.2.2 The Customer shall comply with:

(a) all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

(b) the terms of this agreement.

1.2.3 The Customer warrants, represents and undertakes, that:

(a) with respect to data being provided to or accessed by Supplier for the performance of the Services under this agreement, such data shall have been sourced by the Customer in all respects in compliance with Data Protection Laws, including in terms of its collection, storage and processing, which for the avoidance of doubt includes the Customer providing all required fair processing information to, and obtaining all necessary consents from, Data Subjects;

(b) all instructions given by it to Supplier in respect of Personal Data shall at all times be in accordance with Data Protection Laws;

(c) it has undertaken due diligence in relation to Supplier's processing operations, and it is satisfied that:

(i) Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage Supplier to process the Protected Data; and

(ii) Supplier has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

1.2.4 The Customer shall not unreasonably withhold, delay or condition its agreement to any Change requested by Supplier in order to ensure the Services and Supplier (or any Sub-Processor) can comply with Data Protection Laws.

1.3 **Details of processing and instructions**

1.3.1 Insofar as Supplier processes Protected Data on behalf of the Customer, Supplier:

(a) unless required to do otherwise by Applicable Law, shall, and shall take steps to ensure each person acting under its authority shall, process the Protected Data only on and in accordance with the Customer's documented instructions as set out in this clause 1 and Schedule 1.3.1 (*Data Processing Details*), as updated from time to time in accordance with the Change Control Procedure ("**Processing Instructions**");

(b) if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data unless Applicable Law prohibits such information on important grounds of public interest; and

(c) shall inform the Customer if Supplier becomes aware of a Processing Instruction that, in Supplier's opinion, infringes Data Protection Laws:

(i) provided that doing so shall be without prejudice to clauses 1.2.2 and 1.2.3;

(ii) it being agreed that to the maximum extent permitted by mandatory law, Supplier shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs,

expenses or liabilities (including any Data Processing Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following Supplier informing the Customer of an infringing Processing Instruction; and

(iii) it being understood that this clause 1.3.1(c) shall only apply from the GDPR Date.

1.3.2 The processing of Protected Data to be carried out by Supplier under this agreement shall comprise the processing set out in Schedule 1.3.1 (*Data Processing Details*), as may be updated from time to time in accordance with the Change Control Procedure.

1.4 **Technical and organisational measures**

1.4.1 Supplier shall implement and maintain, at its cost and expense, the technical and organisational measures:

(a) in relation to the processing of Protected Data by Supplier, as set out in and substantially in compliance with Schedule 1.3.1 (*Data Processing Details*) and the Security Measures; and

(b) from the GDPR Date, taking into account the nature of the processing, to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

1.4.2 Any additional technical and organisational measures requested by the Customer shall be at the Customer's cost and expense and only to the extent reasonably possible to be implemented.

1.5 **Security of processing**

1.5.1 Supplier shall, in respect of the Protected Data processed by it under this agreement comply with the requirements regarding security of processing set out in Data Protection Laws as applicable to Data Processors and in this agreement including clause 1.4.

1.6 **Using staff and other processors**

1.6.1 Supplier shall not engage any Sub-Processor for carrying out any processing activities in respect of the Protected Data without first appointing Sub-Processors under a written contract containing materially the same obligations as under this clause 1.

1.6.2 Supplier shall take reasonable steps to ensure that all Supplier Personnel who have access to personal data are reliable and, from the GDPR Date, that all Supplier Personnel authorised to process Protected Data are subject to a binding written contractual obligation with Supplier to keep the Protected Data confidential except where disclosure is required in accordance with Applicable Law, in which case Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure.

1.7 **Assistance with the Customer's compliance and Data Subject rights**

1.7.1 Supplier shall refer all Data Subject Requests it receives to the Customer within three Business Days of actual receipt of the request, provided that, if the number of Data Subject Requests exceeds 20 per calendar month, the Customer shall pay Supplier's charges calculated on a time and materials basis at Supplier's rates set out in Schedule 1.3.1 (*Data Processing Details*) for recording and referring the Data Subject Requests in accordance with this clause 1.7.1 (Charges).

1.7.2 From the GDPR Date, Supplier shall provide such reasonable assistance as the Customer reasonably requires, taking into account the nature of processing performed by and the information available to Supplier, to comply with the Customer's obligations under Data Protection Laws with respect to the Services as they relate to:

(a) security of processing;

(b) DPIAs;

(c) prior consultation with a Supervisory Authority regarding high risk processing; and

(d) notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay Supplier's Charges for providing assistance under this clause 1.7.2

1.8 **International data transfers**

1.8.1 The Customer agrees that Supplier may transfer Protected Data for the purposes of providing services to Customer to countries outside the European Economic Area (EEA) or to any international organisation(s) (individually or collectively, an "International Recipient"), provided all transfers by Supplier of Protected Data to an International Recipient and any onward transfer shall to the extent required under Data Protection Laws be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The foregoing sentence shall constitute a Customer instructions with respect to international data transfers for the purposes of clause 1.3.1.

1.9 **Records, information and audit**

1.9.1 Supplier shall maintain, in accordance with Data Protection Laws binding on Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

1.9.2 Supplier shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate Supplier's compliance with the obligations of Data Processors under Data Protection Laws, and allow for and contribute to audits, including inspections, by the Customer or another auditor mandated by the Customer for this purpose, subject to the Customer:

(a) giving Supplier reasonable prior notice of such information request, audit or inspection being required by the Customer;

(b) ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential, save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law;

(c) ensuring that such audit or inspection is undertaken during normal business hours, with minimal disruption to Supplier's business, a Sub-Processor's business, or the business of other customers of Supplier; and

(d) paying Supplier's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.

1.10 **Notification of Personal Data Breaches and Complaints**

1.10.1 In respect of any Personal Data Breach involving Protected Data, Supplier shall, without undue delay:

(a) notify the Customer of the Personal Data Breach; and

(b) provide the Customer with details of the Personal Data Breach.

1.10.2 Each party shall promptly, and in any event within three Business Days, inform the other if it receives a Complaint and provide the other party with full details of such Complaint.

1.11 **Deletion or return of Protected Data and copies**

1.11.1 Supplier shall, at the Customer's written request, either delete or return all the Protected Data to the Customer within a reasonable time after the end of the provision of the relevant Services related to processing, and delete any other existing copies thereof unless storage of any data is required by Applicable Law and, where this is the case, Supplier shall inform the Customer of any such requirement.

1.12 **Liability, indemnities and compensation claims**

1.12.1 The Customer shall indemnify and keep indemnified Supplier in respect of all Data Processing Losses suffered or incurred by, awarded against or agreed to be paid by, Supplier and any Sub-Processor arising from or in connection with any:

(a) non-compliance by the Customer with the Data Protection Laws;

(b) processing carried out by Supplier or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or

(c) breach by the Customer of any of its obligations under this clause 1,

except to the extent Supplier is liable under clause 1.12.2.

1.12.2 Supplier shall be liable for Data Processing Losses howsoever arising, whether in contract, tort (including negligence) or otherwise under or in connection with this agreement:

(a) only to the extent caused by the processing of Protected Data under this agreement and directly resulting from Supplier's breach of this clause 1; and

(b) in no circumstances for any portion of the Data Processing Losses (or the circumstances giving rise to them) contributed to or caused by any breach of this agreement by the Customer (including a breach of clause 1.3.1(c)(ii)).

1.12.3 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with notice and full details of such claim, and each party shall:

(a) make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party, which consent shall not be unreasonably withheld, conditioned or delayed; and

(b) consult fully with the other party in relation to any such action, but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under this agreement for paying the compensation.

1.12.4 The parties agree that the Customer shall not be entitled to claim back from Supplier any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify Supplier in accordance with clause 1.12.1.

1.12.5 This clause 1.12 is intended to apply to the allocation of liability for Data Processing Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

(a) to the extent not permitted by Applicable Law (including Data Protection Laws); and

(b) that it does not affect the liability of either party to any Data Subject.

APPENDIX 1

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY TELETRAC NAVMAN (UK) LTD.

TECHNICAL MEASURES

1. Inventory and Control of Hardware Assets	Actively manage all hardware devices on the network.
2. Inventory and Control of Software Assets	Audit software on laptops, PCs and workstations the network so that only authorized software is installed.
3. Controlled Use of Administrative Privileges	Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data.
4. Email and Web Browser Protections	Deploy automated controls to minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems or content.
5. Limitation and Control of Network Ports, Protocols, and Services	Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimize windows of vulnerability and exposure available to attackers.
6. Data Recovery Capabilities	Maintain processes and tools to properly back up personal data with a proven methodology to ensure the confidentiality, integrity, availability, and recoverability of that data.
7. Boundary Defenses	Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data.
8. Data Protection	Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the confidentiality and integrity of personal data.
9. Controlled Access Based on the Need to Know	Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical or controlled assets based on an approved classification.
10. Wireless Access Control	Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.
11. Account Monitoring and Control	Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimize opportunities for unauthorized, inappropriate, or nefarious use.

ORGANISATIONAL MEASURES

Organisational Measures to Ensure Security of Processing	
1. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises	Test the overall strength of the organisation's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organisation's privacy and personal data protections.
2. Physical Security and Entry Control	Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits.

SCHEDULE 1.3.1

DATA PROCESSING DETAILS

1. SUBJECT-MATTER OF PROCESSING:

   Vehicle and driver information

2. DURATION OF THE PROCESSING:

   For the term of Customer's contract with Supplier

3. NATURE AND PURPOSE OF THE PROCESSING:

   To enable the provision of Services to Customer by Supplier

4. TYPE OF PERSONAL DATA:

   Employee names and contact details, location data, driving behaviour and related.

5. CATEGORIES OF DATA SUBJECTS:

   Customers and their employees

6. ADDITIONAL INSTRUCTIONS

   a) Authorisations

   Supplier affiliates.

   b) Technical and organisational security measures

   See Appendix 1, which shall form a part of this Schedule 1.3.1

   c) Charges

   £100 per hour.