Annex 1 to Teletrac Navman (UK) Ltd contracts with Suppliers and other third parties

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 Protection Laws**" means any law, enactment, regulation, regulatory policy, by law, ordinance or subordinate legislation **OR** Applicable Law relating to the processing, privacy, and use of Personal Data, as applicable to TTN , the Supplier and/or the Services, including:

(a) in the UK:

(i) the Data Protection Act 1998 ("**DPA 1998**") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any laws or regulations implementing Council Directives 95/46/EC ("**Data Protection Directive**") or 2002/58/EC ("**ePrivacy 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 the ePrivacy Directive, and all relevant Member State laws or regulations giving effect to or corresponding with any of them; and

(c) any judicial or administrative interpretation of any of the above, and any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority;

"**Data Processing Losses**" means all liabilities and amounts, 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, which includes emotional distress);

(b) loss or damage to reputation, brand or goodwill;

(c) to the extent permitted by Applicable Law:

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

(ii) compensation paid to a Data Subject; and

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

(d) the costs of loading TTN data and replacement of TTN materials and equipment, to the extent the same are lost, damaged or destroyed, and any loss or corruption of TTN data, including the costs of rectification or restoration of TTN data;

"**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 or privacy impact assessment (as defined or used in the Data Protection Laws, including relevant guidance from Supervisory Authorities);

"**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 made available or accessible by or on behalf of TTN , or otherwise obtained in connection with the performance of the Supplier's obligations under this agreement;

"**Security Measures**" means TTN's security policies and measures (including IT policies and measures) for the protection of Personal Data issued to Supplier by TTN from time to time, which as at the date hereof are as specified in Appendix 1.

"**Sub-Processor**" means another Data Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of TTN , and authorised by TTN in accordance with clause 1.6;

"**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**" and 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 any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including particularly the GDPR and/or the Revised UK DP Law) and the equivalent terms defined in such Applicable Laws, once in force and applicable;

A.2.3 clause 1 (below) (Data Protection) shall survive termination (for any reason) or expiry of this agreement (or of any of the Services);

---

1. DATA PROTECTION

1.1 Data Controller and Appointment of Data Processor

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

1.2 Compliance with Data Protection Laws and obligations

1.2.1 The Supplier shall comply with 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.

1.2.2 The Supplier shall procure that any Sub-Processor that has access to Protected Data shall comply with the Supplier's obligations under this clause 1.

1.2.3 TTN shall comply with all Data Protection Laws in respect of the performance of its obligations under this agreement.

1.3 Details of processing and instructions

1.3.1 The processing to be carried out by the Supplier under this agreement shall comprise the processing set out in Schedule 1.3.1 (*Data Processing Details*), as updated from time to time by TTN or in the case of a purchase order the relevant data processing undertaken by Supplier in furtherance of meeting its obligations towards TTN.

1.3.2 Insofar as the Supplier processes Protected Data on behalf of TTN, the Supplier:

(a) unless required to do otherwise by Applicable Law, shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with TTN's documented instructions as set out in this clause 1 and Schedule 1.3.1 where applicable *(Data Processing Details)*, and as updated from time to time by the written agreement of the parties ("**Processing Instructions**");

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

(c) shall immediately inform TTN in writing if, in the Supplier's reasonable opinion, a TTN instruction infringes Data Protection Laws and explain the reasons for such opinion.

1.4 Technical and organisational measures

1.4.1 The Supplier shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the processing of Protected Data by the Supplier:

(a) such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;

(b) so as to ensure a level of security in respect of Protected Data processed by it appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed; and

(c) without prejudice to clause 1.8, insofar as is possible, to assist TTN in the fulfilment of TTN's obligations to respond to Data Subject Requests relating to Protected Data.

1.5 Security of processing

1.5.1 Without prejudice to clause 1.4.1(b), the Supplier shall, in respect of all Protected Data processed by it, comply with the requirements regarding security of processing set out in Data Protection Laws and in this agreement and all relevant TTN Policies. The Supplier shall ensure that the Security Measures are the minimum security standards governing Supplier's processing of the Protected Data.

1.6 Using other Sub-Processors

1.6.1 The Supplier shall not engage any third party to process the Protected Data without TTN's prior written consent.

1.6.2 If TTN gives its consent for such third party to act as a Sub-Processor, the Supplier shall, prior to any processing of Protected Data by the Sub-Processor, appoint the Sub-Processor under a binding written contract, with enforceable data protection obligations on the same terms, or terms more onerous than those, that apply to the Supplier under this clause 1 ("**Processor Contract**"), including in particular that the Sub-Processor:

(a) provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Laws; and

(b) must obtain TTN's prior written consent and comply with the conditions referred to in this clause 1.6 for engaging another Data Processor.

1.6.3 The Supplier shall:

(a) promptly upon request by TTN provide the relevant details of any such Processor Contract to TTN;

(b) where that Sub-Processor fails to fulfil its data protection obligations in accordance with the Processor Contract, remain fully liable to TTN for the performance of that Sub-Processor's obligations; and

(c) immediately cease using a Sub-Processor to process Protected Data upon receiving written notice from TTN requesting that the Sub-Processor ceases processing Protected Data for security reasons or concerns about the Sub-Processor's ability to carry out the relevant processing in compliance with Data Protection Laws or this agreement.

1.7 Personnel requirements

1.7.1 The Supplier shall:

(a) ensure that Supplier Personnel (and shall procure that Sub-Processor personnel) processing Protected Data have entered into a binding contractual obligation with the Supplier to keep the Protected Data confidential (except where disclosure is required by Applicable Law, in which case the Supplier shall, where practicable and not prohibited by such Applicable Law, notify TTN of any such requirement before such disclosure); and

(b) ensure the reliability of the Supplier Personnel processing Protected Data and further ensure that the Supplier Personnel processing Protected Data receive adequate training on compliance with this clause 1 and the Data Protection Laws applicable to the processing.

1.8 Data Subject rights

1.8.1 The Supplier shall:

(a) at no cost to TTN, record and then refer all Data Subject Requests which the Supplier receives to TTN within three days of receipt of the Data Subject Requests;

(b) at its cost and expense, provide such information and cooperation and other assistance as TTN requests in relation to a Data Subject Request within the timescales reasonably required by TTN ; and

(c) not respond to any Data Subject Request without TTN's prior written authorisation.

1.9 Assistance with TTN's compliance

1.9.1 The Supplier shall, at its own cost and expense, provide such information, cooperation and other assistance as TTN requests to ensure TTN's compliance with its obligations under Data Protection Laws, including with respect to:

(a) security of processing;

(b) any remedial action and notifications to be taken in response to any Personal Data Breach or Complaint, including (subject in each case to TTN's prior written authorisation) regarding any notification of the Personal Data Breach to Supervisory Authorities and/or communication to affected Data Subjects, including in accordance with clause 1.13;

(c) DPIAs, by promptly providing such information and cooperation as TTN may reasonably require for the purpose of assisting TTN in carrying out a DPIA, and periodic reviews to assess if the processing of Protected Data is performed in compliance with the outcomes of the DPIA;

(d) prior consultation with a Supervisory Authority regarding high risk processing, by promptly and in consultation with TTN :

(i) providing such information and cooperation as TTN or a Supervisory Authority requests for the purpose of assisting in any consultation by TTN with the Supervisory Authority; and

(ii) complying with any advice by a Supervisory Authority concerning the Supplier's processing activities related to this agreement.

1.10 International data transfers

1.10.1 The Supplier shall not (and shall procure that any Sub Processor or subcontractor shall not) transfer, or allow the onward transfer of, any Protected Data to any country outside the European Economic Area ("**EEA**") or to any international organisation (individually and collectively, an "**International Recipient**") without TTN's prior written consent.

1.10.2 If TTN consents to the transfer of Protected Data to an International Recipient, the Supplier shall ensure that such transfer (and any subsequent onward transfer):

(a) is pursuant to a written contract including equivalent or more onerous obligations on the Sub-Processor in respect of the Protected Data (in particular relating to security and confidentiality) as apply to the Supplier under this clause 1;

(b) is effected by way of Appropriate Safeguards, the form of which being subject to TTN's prior written approval (which shall not be unreasonably withheld or delayed);

(c) complies with clause 1.2.1 and any requirements specified in Schedule 1.3.1 as applicable (*Data Processing Details*) including the Security Measures; and

(d) otherwise complies with Data Protection Laws.

1.11 Records

1.11.1 The Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of TTN, containing such information as TTN may reasonably require, including:

(a) the name and contact details of the Data Processor(s) and of each Data Controller on behalf of which the Data Processor is acting, and of the Supplier's representative and data protection officer (if any);

(b) the categories of processing carried out on behalf of each Data Controller;

(c) where applicable, details of transfers of Protected Data to an International Recipient, including the identification of that International Recipient and the relevant countries to which such data is transferred, and details of the Appropriate Safeguards used; and

(d) a general description of the technical and organisational security measures referred to in clause 1.4.1(b).

1.12 Compliance, information and audit

1.12.1 The Supplier shall (and shall procure that its Sub-Processors) make available to TTN on request in a timely manner (and in any event within three days):

(a) copies of the records under clause 1.11; and

(b) such other information as TTN reasonably requires to demonstrate the Supplier's compliance with its obligations under Data Protection Laws and this agreement, including sufficiently detailed information about the technical and organisational measures that are implemented and maintained by the Supplier.

1.12.2 The Supplier shall (and shall procure that its Sub-Processors shall) allow for and contribute to audits, including inspections, conducted by TTN or another auditor mandated by TTN for the purpose of demonstrating compliance by the Supplier with its obligations under Data Protection Laws and under this clause 1, including allowing reasonable access for TTN or such other auditor to:

(a) the facilities, equipment, premises and sites on which Protected Data and/or the records referred to in clause 1.11 are held, and to any other equipment or facilities used in the provision of the Services (in each case whether or not owned or controlled by the Supplier); and

(b) the Supplier Personnel,

provided that TTN shall, where practicable, give the Supplier reasonable prior notice of such audit and/or inspection and conduct the same during normal business hours.

1.12.3 If any audit or inspection reveals a material noncompliance by the Supplier with its obligations under Data Protection Laws or a breach by the Supplier of its data protection obligations under this agreement, the Supplier shall promptly on request:

(a) pay the reasonable costs of TTN or its mandated auditors for the audit or inspection; and

(b) resolve (and shall procure that its Sub-Processors likewise resolve), at its own cost and expense, all instances of data protection or security noncompliance discovered by TTN and reported to the Supplier that reveal a breach or potential breach by the Supplier (or a Sub-Processor) of its obligations under this clause 0.

1.12.4 TTN may share any notification, details, records or information provided by or on behalf of the Supplier under this clause 1.12 or clause 1.13 with its respective affiliates, professional advisors, and any Supervisory Authority.

1.12.5 If the Supplier (or a Sub-Processor) is in breach of its obligations under this clause 0, TTN may suspend the transfer of Protected Data to the Supplier until the breach is remedied.

1.13 Notification of Personal Data Breaches and Complaints

1.13.1 In respect of any actual or suspected Personal Data Breach involving the Supplier or a Sub-Processor, the Supplier shall:

(a) notify TTN of the Personal Data Breach without undue delay, but in no event later than twelve hours after becoming aware of such Personal Data Breach; and

(b) provide TTN without undue delay, wherever possible no later than twenty-four hours after becoming aware of such Personal Data Breach, with such details as TTN requires regarding:

(i) the nature of such Personal Data Breach, including the categories and approximate numbers of Data Subjects and Personal Data records concerned;

(ii) any investigations into such Personal Data Breach;

(iii) the likely consequences of such Personal Data Breach; and

(iv) any measures taken, or that the Supplier recommends to take, to address such Personal Data Breach, including to mitigate its possible adverse effects and prevent the re-occurrence of such Personal Data Breach or a similar breach,

provided that, without prejudice to the above obligations, if the Supplier cannot provide all these details within the aforesaid timeframe, it shall in any event before the end of said timeframe provide TTN with its reasons for the delay and an expectation for when it reasonably expects to be able to provide TTN with such details.

1.13.1 The Supplier shall promptly and in any event within two days inform TTN if it receives a Complaint and provide TTN with full details of such Complaint.

1.14 Deletion or return of Protected Data and copies

1.14.1 The Supplier shall without delay:

(a) at TTN's written request, either securely delete or securely return all the Protected Data to TTN in such form as TTN reasonably requests, after the earlier of:

(i) the end of the provision of the relevant Services related to processing; or

(ii) once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this agreement; and

(b) securely delete all other existing copies of the Protected Data, except only for those copies that are required to be stored by Applicable Law and, in which case, the Supplier shall inform TTN of any such requirement; and

(c) upon full performance of its obligations unde this clause 1.14, provide TTN with a written declaration of such performance.

1.15 Liability and indemnities

1.15.1 The Supplier shall indemnify and keep indemnified TTN in respect of all Data Processing Losses suffered or incurred by, awarded against or agreed to be paid by, TTN or any affiliate thereof, arising from or in connection with:

(a) any breach by the Supplier of its obligations under this clause 1 or of Data Protection Laws; or

(b) the Supplier (or any person acting on its behalf) acting outside or contrary to the lawful Processing Instructions of TTN in respect of the processing of Protected Data.

1.15.2 This clause 1.15 is intended to apply to the allocation of liability for Data Protection 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
SECURITY MEASURES

DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY SUPPLIER

Technical Measures

1. Inventory and Control of Hardware Assets	Actively manage all hardware devices on the network so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.
2. Inventory and Control of Software Assets	Actively manage all software on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. 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.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Implement and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyse audit and security logs of events that could help detect, understand, or recover from a possible attack.
7. Email and Web Browser Protections	Deploy automated controls to minimise the attack surface and the opportunities for attackers to manipulate human behaviour through their interaction with web browsers and email systems or content.
8. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimising the use of automation to enable rapid updating of defense, data gathering, and corrective action.
9. 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 minimise windows of vulnerability and exposure available to attackers.
10. 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.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12. Boundary Defenses	Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data.

13. 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.
14. 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.
15. 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.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimise opportunities for unauthorised, inappropriate, or nefarious use.

Organisational Measures

1. Implement a Comprehensive Information Security Programme	Through the implementation of a Comprehensive Information Security Programme (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure: • security, confidentiality and integrity of personal data • protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud • that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller.
2. Implement a Security Awareness and Training Programme	For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programmes.
3. Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

SCHEDULE 1.3.1 *[NOT APPLICABLE FOR PURCHASE ORDERS]*
DATA PROCESSING DETAILS

1. SUBJECT-MATTER OF PROCESSING:

INSERT

2. DURATION OF THE PROCESSING:

INSERT

3. NATURE AND PURPOSE OF THE PROCESSING:

INSERT

4. TYPE OF PERSONAL DATA:

INSERT

5. CATEGORIES OF DATA SUBJECTS:

INSERT

6. ADDITIONAL INSTRUCTIONS

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

Insert any additional instructions, e.g., Details of pre-approved international transfers or pre-approved Sub-Processors