DATA PROCESSING TERMS

In order that you as a service provider and data processor (referred to as "**Processor**" or "**you**" or "**your**") may provide or continue to provide certain services (the "**Services**") to us, the Business and data controller (referred to as "**Business**" or "**we**", "**us**" or "**our**"), you have agreed that these data processing terms ("**Terms**") shall apply (notwithstanding any other terms and conditions applicable to the delivery of the Services to the contrary) in order to address the compliance obligations imposed upon the Businessand its Clients pursuant to the Data Protection Law. These Terms shall constitute a separate agreement or they may be incorporated by reference in the relevant Services agreement, as the case may be.

BY ACCEPTING ANY MATERIALS FROM THE BUSINESSOR OTHERWISE COMMENCING THE SERVICES ("EFFECTIVE DATE"), YOU AGREE THAT THE PROCESSOR WILL PROCESS BUSINESSPERSONAL DATA IN ACCORDANCE WITH THESE TERMS, WHICH YOU HEREBY ACCEPT FOR AND ON BEHALF OF THE PROCESSOR.

NOW IT IS HEREBY AGREED as follows:

1. DEFINITIONS

1.1. In this Agreement, capitalised words shall have the meaning as set out below or, as the case may be, elsewhere in this Agreement:

"Affiliate"	means any entity that directly or indirectly controls, is controlled by, or is under common control with, a party from time to time during the Term;
"Data Protection Law"	means the data privacy laws applicable to the processing in connection with the Services, including, where applicable, the Directive 95/46/EC, as amended or replaced by any subsequent Regulation, Directive or other legal instrument of the European Union including by the General Data Protection Regulation or similar law, or the applicable data privacy laws of any other relevant jurisdiction;
"Client"	means any client of the Business;
"Contractual Clauses"	means the standard contractual clauses of the European Commission for the transfer of personal data across borders, as amended or replaced from time to time, or any equivalent set of contractual clauses approved for use under Data Protection Law; and
"BusinessPersonal Data"	means the personal data processed by Processor in connection with the Services on behalf of the Businessduring the Term. The processing may include activities auxiliary to our services, such as postal, courier, legalisation, translation, hosting, administrative and other services. This will include names and other information about data subjects included in Client materials.

1.2. The words "**data subject**", "**personal data**", "**processing**" and variations, "**controller**" and "**processor**" shall have the meaning attributed to them in Data Protection Law.

2. APPOINTMENT

2.1. The Businessis designated by its Clients, Client Affiliates and BusinessAffiliates (collectively "**Instructing Parties**") to provide and manage various services, including the Services on their behalf. Accordingly, BusinessPersonal Data may contain personal data in relation to which Instructing Parties are controllers. Businessconfirms that it is authorised to communicate to Processor any instructions or other requirements on behalf of Instructing Parties in respect of processing of BusinessPersonal Data by Processor in connection with the Services.

2.2. Processor is appointed by Businessto process BusinessPersonal Data on behalf of the Businessand/or the Instructing Parties, as the case may be, as is necessary to provide the Services or as otherwise agreed by the parties in writing.

3. DURATION

The Terms shall commence on the Effective Date and shall continue in full force and effect until such time as all Services have ceased and all BusinessPersonal Data in the Processor's possession or within its reasonable control (including those held by a Subprocessor) has been returned or destroyed (the "**Term**").

4. DATA PROTECTION COMPLIANCE

4.1. In relation to its processing of BusinessPersonal Data, save as otherwise required by law, you agree to:

(a) process BusinessPersonal Data only as required in connection with the Services and in accordance with our documented lawful instructions from time to time;

(b) inform us if, in your opinion, an instruction infringes Data Protection Law;

(c) ensure that all personnel authorised by you to process BusinessPersonal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(d) implement appropriate technical and organisational measures to appropriately safeguard BusinessPersonal Data having regard to the nature of the personal data which is to be protected and the risk of harm which might result from any Security Breach (as defined below), at a minimum the measures set out in the Schedule;

(e) promptly inform us of any data subject requests under Data Protection Law or regulatory or law enforcement requests relating to BusinessPersonal Data. You shall not acknowledge or otherwise respond to the subject access request except with our prior written approval, which shall not be unreasonably withheld;

(f) provide such assistance as the Businessmay reasonably require in order to ensure our or the Instructing Parties' compliance with Data Protection Law in relation to data security, data breach notifications, data protection impact assessments and prior consultations with the Information Commissioner's Office or other competent authority;

(g) at our choice, without delay delete or return all BusinessPersonal Data to us, and delete existing copies of all BusinessPersonal Data in the Processor's possession or within its reasonable control (including those held by a Subprocessor); and

(h) make available to Businessinformation reasonably necessary to demonstrate your compliance with these Terms and allow for, and contribute to, audits and inspections carried out by the Business.

5. SUBPROCESSORS

5.1. Processor will sub-contract, outsource, assign, novate or otherwise transfer obligations under these Terms or engage any subcontractors involved in the processing of BusinessPersonal Data (each a "**Subprocessor**") only with Business's prior written consent and subject to clause 5.2.

5.2. When engaging a Subprocessor, Processor will:

(a) carry out reasonable due diligence;

(b) enter into a contract on terms, as far as practicable, same as those in these Terms, and which may include Contractual Clauses to provide

adequate safeguards with respect to the processing of BusinessPersonal Data; and

(c) inform us of any intended changes concerning the addition or replacement of a Subprocessor from time to time. If we object to any such change on reasonable grounds, then acting in good faith the parties will work together to resolve such objection.

6. SECURITY INCIDENTS

6.1. "**Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, BusinessPersonal Data transmitted, stored or otherwise processed.

6.2. Processor will notify the Businesswithout undue delay if Processor aware of any Security Breach.

6.3. Processor will investigate the Security Breach and take reasonable action to identify, prevent and mitigate the effects of the Security Breach. Processor will take such further action as we may reasonably request in order to comply with Data Protection Law.

6.4. Processor may not release or publish any filing, communication, notice, press release, or report concerning any Security Breach ("**Notices**") without our prior written approval; such approval shall not be unreasonably withheld.

7. INTERNATIONAL DATA TRANSFERS

7.1. Processor will ensure that no BusinessPersonal Data are transferred out of either:

(a) the European Economic Area; or

(b) any other territory in which restrictions are imposed on the transfer of BusinessPersonal Data across borders under Data Protection Laws,

without the prior written consent of Businessand subject to clause 7.2.

7.2. Businesswill ensure that Contractual Clauses or other applicable transfer mechanism, such as EU-US Privacy Shield Framework in relation to EU-US transfers, is in place to ensure adequate level of data protection.

8. INDEMNITY

Notwithstanding any provisions of the relevant Services agreement to the contrary, Processor shall and hereby agrees to indemnify Businessand Instructing Parties and their officers, employees, agents and subcontractors (each an "**Indemnified Party**") from and against any claims, losses, demands, actions, liabilities, fines, penalties, reasonable expenses, damages and settlement amounts (including reasonable legal fees and costs) incurred by any Indemnified Party as a result of any gross negligence or wilful breach by Processor of these Terms.

9. MISCELLANEOUS

9.1. Clause and other headings in these Terms are for convenience only and shall not affect the meaning or interpretation of these Terms.

9.2. To the extent of any conflict, these Terms shall prevail over any Services agreement or other agreement.

9.3. Nothing in these Terms will exclude or limit the liability of either party which cannot be limited or excluded by applicable law. Subject to the foregoing sentence, (i) these Terms, including any appendices, constitutes the entire agreement between the parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations and discussions of the parties relating to its subject matter; and (ii) in relation to the subject matter of these Terms neither party has relied on, and neither party will have any right or remedy based on, any statement, representation or warranty, whether made negligently or innocently, except those expressly set out in these Terms.

9.4. Processor shall agree any amendment to these Terms that may be required from time to time for us and Instructing Parties to comply with any amended Data Protection Laws.

9.5. All notices of termination or breach must be in English, in writing and addressed to the other party's primary contact person or legal department. Notice will be treated as given on receipt, as verified by a valid receipt or electronic log. Postal notices will be deemed received 48 hours from the date of posting by recorded delivery or registered post.

9.6. The provisions of these Terms are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of these Terms shall remain in full force and effect.

9.7. These Terms are governed by English law and the parties submit to the exclusive jurisdiction of the English courts in relation to any dispute (contractual or non-contractual) concerning these Terms save that either party may apply to any court for an injunction or other relief to protect its property or confidential information.

SCHEDULE: Security measures

Processor shall put in place the following measures, as applicable.

Minimum technical measures

- Firewalls which are properly configured and using the latest software;
- user access control management;
- unique passwords of sufficient complexity and regular expiry on all devices;
- secure configuration on all devices;
- regular software updates, if appropriate, by using patch management software;
- timely decommissioning and secure wiping (that renders data unrecoverable) of old software and hardware;
- real-time protection anti-virus, anti-malware and anti-spyware software;
- https;
- encryption of all portable devices ensuring appropriate protection of the key;
- encryption of personal data in transit by using suitable encryption solutions;
- multi-factor authentication for remote access;
- WPA-TKIP secured WiFi access;
- delinquent web filtering and other appropriate internet access restrictions;
- intrusion detection and prevention systems;
- appropriate and proportionate monitoring of personnel; and
- data backup and disaster recovery measures and procedures.

Minimal organisational measures

- Vet all personnel including staff, contractors, vendors and suppliers (including Subprocessors) on continuous basis;
- non-disclosure agreements used with all personnel;
- regular training of all personnel on confidentiality, data processing obligations, identification of Security Breaches and risks;
- apply principle of least authority, including a restricted or strictly controlled transit of data and material outside of office;
- physical security on premises including reception or front desk, security passes, clean desk policy, storage of documents in secure cabinets, secure disposal of materials, CCTV, etc.;
- apply appropriate policies including Information Security Policy, Data Protection Policy, BYOD, Acceptable Use Policy; limited and monitored personal use of work resources, as appropriate.