DATA PROTECTION TERMS ("DP TERMS")

1. DEFINITIONS AND INTERPRETATION

For the purpose of these DP Terms, the following terms have the meanings ascribed to them (and are in addition to, and shall prevail over, the definitions at Clause 1.1 of the Contract):

"**Applicable EU Law**" means any law of the European Union (or the law of one of the Member States of the European Union or the United Kingdom));

"**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 of this Contract.

"**Approved Sub-contractor**" means a sub-contractor appointed in accordance with paragraph 9;

"**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", and "**Processor**" shall have the meanings given to them under Data Protection Laws(whereby: (i) "Process" and "**Processed**" shall be construed accordingly; (ii) any references to "**Personal Data**" shall include a reference to "**Sensitive Personal Data**"; and (iii) any references to "**Personal Data Breach**" shall include a breach of paragraph 3.1.3);

"Contract" means the binding agreement between the Controller and Processor of which these Data Protection Terms form part;

"Contract Year" means a period of 12 months (or shorter, if relevant, to the date of termination), commencing on the start date of the Contract ("Commencement Date") and/or each subsequent period of 12 months (or shorter, if relevant, to the date of termination) commencing on the date falling on each anniversary of the Commencement Date thereafter.

"**Customer Security Requirements**" means the Customer's prevailing IT security standards and requirements, as are set out in the Customer's Information Security Terms (as defined in the Contract);

"**Data Processing Terms**" means the terms in these DP Terms;

"**Data Protection Laws**" means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (each as amended, consolidated or re-enacted from time to time) which relates to data protection to which a Party is subject, including the Data Protection Act 2018, UK GDPR and the EU GDPR (known as the "GDPR" as the context requires); ; and (b) any code of practice or guidance published by the ICO and/or European Data Protection Board (as applicable) from time to time**;**

"**Data Processing Particulars**" means, in relation to any Processing:

(i) the subject matter and duration of the Processing;

(ii) the nature and purpose of the Processing;

(iii) the type of Personal Data being Processed; and

(iv) categories of Data Subjects;

and which are set out in a Schedule in the Contract;

"**Data Protection Impact Assessment**" means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by Article 35 of the UK GDPR;

"**Data Subject Request**" means an actual or purported request, notice or complaint from (or on behalf of) a Data Subject exercising his rights under the Data Protection Laws;

"**Data Transfer**" means transferring the Personal Data to, and/ or accessing the Personal Data from

and/ or Processing the Personal Data within, a jurisdiction or territory that is a Restricted Country;

"**Data Transfer Risk Assessment**" means a risk assessment completed by the Supplier in the form of Appendix 2;

"**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data;

"Good Industry Practice" means, at any time, the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of services similar to the Services to a customer like the Customer, such supplier seeking to comply with its contractual obligations in full and complying with all applicable laws (including the Data Protection Laws);

"**Losses**" means, whether arising in contract, tort (including negligence), breach of statutory duty or otherwise:

(i) losses;
(ii) liabilities;
(iii) damages;
(iv) costs;
(v) charges;
(vi) expenses,

including without limitation to the generality of this term:

(1) legal fees, on a solicitor/client basis;
(2) other professional charges and expenses;
(3) disbursements;
(4) costs of investigation including forensic investigation;
(5) cost of breach notification including notifications to the Data Subject;
(6) cost of complaints handling including providing Data Subjects with credit reference checks, setting up contact centres (eg call centres), producing end customer communication materials, provision of insurance to end customers (eg identity theft), reimbursement of costs incurred by end customers (eg changing locks);
(7) costs of claims;
(8) cost of litigation;
(9) costs of settlement including ex gratia payments;
(10) judgment interest; and
(11) penalties including fines levied by the Regulator;

"**Model Clauses**" means, as applicable, the form of clauses (i) contained in EU Commission Decision 2010/87/EU of 5 February 2010, or such other replacement, amended or successor clauses approved by the Regulator from time to time;

"**Near Miss**" means a security incident involving Personal Data that is corrected or remediated by the Supplier (or any Approved Sub-contractor) at the last possible instant before becoming an actual Personal Data Breach, where such correction or remediation identifies a material application security vulnerability or other deficiencies in the security measures that the Supplier (or the relevant Approved Sub-contractor) has put in place in accordance with paragraph 3.1.3;

"**Permitted Purpose**" means the purpose of the Processing as set out in more detail in the Data Processing Particulars;

"**Personal Data Breach Particulars**" means the information that must be included in a Personal Data Breach notification, as set out in Article 33(3) of the UK GDPR;

"**Regulator**" means the UK Information Commissioner's Office (including any successor or replacement body);

"**Regulator Correspondence**" means any correspondence or communication (whether written or verbal) from the Regulator in relation to the Processing of the Personal Data;

"Restricted Country" means a country, territory or jurisdiction outside of the UK which is not deemed to provide adequate protection in accordance with Article 45(1) of the UK GDPR or in respect of which no adequacy regulations exist;

"**Security Requirements**" means the requirements regarding the security of the Personal Data, as set out in the Data Protection Laws (including, in particular, the seventh data protection principle of the Act and/ or the measures set out in Article 32(1) of the UK GDPR (taking due account of the matters described in Article 32(2) of the UK GDPR)) as applicable, [and (b) the Customer Security Requirements];

"**Sensitive Personal Data"** means Personal Data that reveals such categories of data as are listed in Article 9(1) of the UK GDPR;

"**Supplier Personnel**" means all persons engaged or employed from time to time by the Supplier in connection with the Contract, including employees, consultants, contractors and permitted agents; and

"**Third Party Request**" means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation;

"**UK GDPR**" means EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2. PARTIES' ROLES UNDER THE DATA PROTECTION LAWS AND APPLICATION OF THIS AGREEMENT

2.1 These Data Processing Terms shall apply to all Personal Data Processed by the Supplier under, or in connection with, the Contract (and a reference to "**Personal Data**" in these Data Processing Terms shall be construed accordingly).

2.2 The Parties shall each Process the Personal Data. The Parties acknowledge that the factual arrangement between them dictates the role of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, the Parties anticipate that the Customer shall act as a Controller and the Supplier shall act as a Processor, as follows:

2.2.1 the Customer shall be a Controller where it is Processing (or instructing the Processing of) Personal Data in relation to the Supplier's performance of Services under the Contract; and

2.2.2 the Supplier shall be a Processor where it is Processing Personal Data in relation to the Permitted Purpose in connection with performing its obligations under this Contract.

2.3 The Supplier shall comply with the Data Protection Laws to the extent that they are applicable to the Services provided by the Supplier or otherwise applicable to the Supplier.

2.4 Each of the Parties acknowledges and agrees that Schedule 4 of the Contract is an accurate description of the Data Processing Particulars.

3. OBLIGATIONS OF THE PROCESSOR

3.1 To the extent that the Supplier is acting as Processor for and on behalf of the Customer in relation to Processing that it is carrying out arising out of, or in connection with, the provision of the Services, the Supplier shall:

3.1.1 fairly and lawfully perform its role as Processor by Processing the Personal Data at all times in accordance with the Data Protection Laws and on behalf of the Customer solely for the purposes of providing the Services, and in the manner specified in the Contract or in any manner expressly required on the instructions of the Customer;

3.1.2 notify the Customer immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it believes (or ought reasonably to have been aware) that:

(a) it is required by Applicable EU Law to act other than in accordance with the instructions of the Customer; or

(b) any of the Customer's instructions under paragraph 3.1.1 infringes any of the Data Protection Laws;

3.1.3 implement and maintain appropriate technical and organisational measures sufficient to comply at least with the obligations imposed on each of the Customer and/ or the Supplier (as applicable) by the Security Requirements;

3.1.4 ensure that all Supplier Personnel in its organisation are made aware of, and act in accordance with, the Supplier's obligations under these Data Processing Terms with regard to the security and protection of the Personal Data and of the Data Subjects;

3.1.5 ensure that each of its agents and subcontractors (including the Approved Sub-contractors) (where relevant) are made aware of the Supplier's safeguarding obligations under these Data Processing Terms with regard to the security and protection of the Personal Data and of the Data Subjects;

3.1.6 only extract, transmit and Process such Personal Data as is appropriate for the provision of the Services and may only Process the Personal Data as is strictly necessary for the performance of its obligations under the Contract and for no other purpose;

3.1.7 without prejudice to the generality of paragraph 3.1.3:

(a) ensure that each of its computers and portable electronic devices (including laptops, tablets, smart phones and USB sticks) that will be used for storing, sending and receiving the Personal Data are appropriately protected against unauthorised use by encryption/passwords and appropriate firewalls/anti-virus packages (with regular and frequent updates being applied) and are physically stored securely when not in use;

(b) ensure that Personal Data transported by portable storage media or by telecommunications network shall be fully encrypted or password protected / sent by secure a virtual private network ("**VPN**") as appropriate and all such data must be wiped from the storage media used for transporting the data or destroyed such that it cannot be recovered once the data has been transferred to the target system;

(c) ensure that any data centre premises on which Personal Data are stored are ISO27001 compliant and compliant with other appropriate security and audit standards throughout the Term;

(d) hold the Personal Data in such a manner that it is capable of being distinguished from other data or information processed by the Supplier;

(e) without prejudice to paragraph 7, ensure that all Supplier Personnel are appropriately vetted and are assigned unique identifiers, and the Supplier shall maintain a comprehensive and complete audit trail detailing which Supplier Personnel have accessed which Personal Data, from where and detailing actions were undertaken in respect of the Personal Data and are made aware of the Supplier's obligations hereunder;

(f) inform the Customer promptly (and in any event within twenty-four (24) hours) upon becoming aware that Personal Data has been used or Processed in a manner which is not expressly permitted by these Data Processing Terms;

(g) inform the Customer (using the address: servicedesk@go-ahead.com and any other such address as may be advised to the Supplier for this purpose throughout the

Termand in any event within twenty-four (24) hours) upon becoming aware of any actual or suspected, threatened or Near Miss Personal Data Breach in relation to the Personal Data, or if the Personal Data is lost (temporarily or permanently) or has the potential to be misused in any way, and shall:

(i) implement:

(1) any measures necessary to restore the security of compromised Personal Data; and

(2) any other measures reasonably requested by the Customer; and

(ii) support the Customer to make any required notifications to any relevant Regulator and affected Data Subjects;

and the parties acknowledge that the operational manner in which the Supplier shall perform its obligation under this paragraph 3.1.7(g) is as set out in paragraph 2 of Appendix 1;

(h) provide a monthly report reflecting the security status which shall be performed by an independent third party: (a) vulnerability scanning, once a quarter in each Contract Year; and (b) penetration testing once each Contract Year;

3.1.8 without prejudice to the generality of Clause 11 of the Contract (Exit Arrangements), except to the extent required by Applicable EU Law, upon the earlier of:

(a) on termination or expiry of this Contract, howsoever caused; and/ or

(b) the date on which the Personal Data is no longer relevant to, or necessary for, the Permitted Purpose;

immediately cease Processing the Personal Data and, at the Customer's option or direction, arrange for the prompt and safe return and/or secure and permanent destruction of all Personal Data, together with all copies in its possession or control and, where requested by the Customer, certify that such destruction has taken place. These DP Terms shall survive termination of the Contract for so long as the Supplier is Processing the Personal Data;

3.1.9 notify the Customer promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or Regulatory Correspondence, and together with such notices, shall provide a copy of such Data Subject Request or Regulatory Correspondence and reasonable details of circumstances giving rise to it. In addition to providing the notice referred to in this paragraph 3.1.9, it shall:

(a) not disclose any Personal Data in response to any Data Subject Request or Regulatory Correspondence without the Customer's prior written consent; and

(b) provide the Customer with all reasonable co-operation and assistance required by the Customer in relation to any such Data Subject Request or Regulatory Correspondence;

3.1.10 allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the Customer (and/ or its representatives, including its appointed auditors), no more than once in any six (6) month period, in order to ascertain compliance with the terms of these Data Processing Terms within twenty (20) Business Days of such a request from the Customer, and shall provide reasonable information, assistance and co-operation to the Customer, including access to relevant Supplier Personnel and/or, on the request of the Customer, provide the Customer with evidence of its compliance with the requirements of these Data Processing Terms;

3.1.11 ensure that non-authorised persons are prevented from entering areas of its premises where Personal Data is Processed. Where this is not possible, all visitors must be escorted at all times;

3.1.12 comply with the obligations imposed on a Processor under the Data Protection Laws; and

3.1.13 assist the Customer (in accordance with Good Industry Practice) to comply with the obligations imposed on the Customer by the Data Protection Laws, including:

(a) compliance with the Security Requirements;

(b) obligations relating to notifications required by the Data Protection Laws to the Regulator and/ or any relevant Data Subjects;

(c) maintaining a written record of the Processing activities that it carries out under these Data Processing Terms, the Customer's instructions referred to in paragraph 3.1.1 and all other records as the Customer may reasonably require and/ or which the Supplier is legally required to keep under Data Protection Laws; and

(d) undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Laws, consulting with the Regulator in respect of any such Data Protection Impact Assessments).

3.1.14 certify each month that no law enforcement or government request for access to Personal Data has been received by the Supplier, its Affiliate or sub-processor, and notify the Customer without delay upon receipt of any such request;

3.1.15 review under the laws of any relevant Restricted Country the legality of any law enforcement or government request for access to Personal Data received by Supplier, its Affiliate or sub-processor, particularly to confirm that the request is within the scope of the powers granted by law to the requesting public authority, and, where there is a ground to do so, to exhaust all available remedies to challenge the request. When challenging a request, the Supplier shall seek interim measures to suspend the request until the court has decided on the merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules of the Restricted Country; and

3.1.16 monitor developments in local laws of each Restricted Country and notify the Customer without delay of any new laws, changes to law or practice, and significant changes in leadership in government bodies that might give rise to a risk of interception or surveillance

4. OBLIGATIONS OF THE CONTROLLER

Each of the Parties respectively undertakes to the other to comply at all times with the Data Protection Laws, and, in particular, the Customer shall ensure that any disclosure of Personal Data made by it to the Supplier is made in accordance with the Data Protection Laws.

5. DATA TRANSFER TO A RESTRICTED COUNTRY

5.1 To the extent that the Supplier is acting as Processor for and on behalf of the Customer in relation to Processing that it is carrying out arising out of, or in connection with, the provision of the Services, it shall not make (nor instruct or permit a third party to make) a Data Transfer unless it:

5.1.1 has first obtained the Customer's prior written consent;

5.1.2 provides, in advance of any such Data Transfer, a Data Transfer Risk Assessment to the Customer; and

5.1.3 has put in place measures to ensure that any transfer is on the basis of and in accordance with the Data Protection Laws (including but not limited to Articles 45 to 49 (inclusive) of the UK GDPR) to ensure the Customer's compliance with the Data Protection Laws, including but not limited to entering into, or procuring that the applicable Approved Sub-contractors enter into, the Model Clauses with the Customer.

6. SUPPLIER PERSONNEL

6.1 To the extent that the Supplier is acting as a Processor for and on behalf of the Customer in relation to Processing that it is carrying out arising out of, or in connection with, the provision of the Services, it shall only disclose the Personal Data to Supplier Personnel where the following conditions have been, and continue to be, satisfied:

6.1.1 the Supplier shall take all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that only such Supplier Personnel required by it to assist it in meeting its obligations under this Contract (which may include assistance with systems administration) and no other Supplier Personnel have access to such Personal Data; and

6.1.2 the Supplier shall ensure that the following conditions shall be met by such Supplier Personnel:

(a) each member of Supplier Personnel shall be subject to adequately clear pre-employment checks that include, as a minimum: employment history for at least the last three (3) years, identity, unspent criminal convictions and right to work (including nationality and immigration status);

(b) each member of Supplier Personnel shall have undergone reasonable levels of training in Data Protection Laws and in the care and handling of Personal Data; and

(c) each member of Supplier Personnel has entered into appropriate contractually-binding confidentiality undertakings.

7. PROCESSOR ACTING OUTSIDE INSTRUCTIONS

7.1 If the Supplier (as a Processor), acts outside the instructions of the Customer (as a Controller), the Supplier shall be in material breach of the Contract and the following shall apply:

7.1.1 if the Customer suffers any Losses as a result of or in connection with such breach, the Supplier shall be liable on an indemnity basis for such losses or damages in accordance with paragraph 8; and

7.1.2 if the Supplier receives a benefit as a result, then regardless of whether or not the Customer has suffered any Losses, the Supplier shall account to the Customer for such benefit.

8. INDEMNITY

8.1 The Supplier shall indemnify on demand and keep indemnified the Customer from and against:

8.1.1 any monetary penalties or fines levied by the Regulator on the Customer;

8.1.2 the costs of an investigative, corrective or compensatory action required by the Regulator, or of defending proposed or actual enforcement taken by the Regulator;

8.1.3 any Losses suffered or incurred by, awarded against, or agreed to be paid by, the Customer pursuant to a claim, action or challenge made by a third party against the Customer (including by a Data Subject); and

8.1.4 except to the extent covered by paragraphs 8.1.1, 8.1.2 and/ or 8.1.3 above, any Losses suffered or incurred, awarded against or agreed to be paid by the Customer,

in each case, arising out of or in connection with a breach by the Supplier of these Data Processing Terms and/ or the Data Protection Laws (and/ or a breach by an Approved Sub-contractor of its sub-contract and/ or the Data Protection Laws).

8.2 Nothing in the Contract shall exclude or limit a party's liability under this paragraph 8.

9. TRANSFERS TO THIRD PARTIES

9.1 If at any time during the Term, the Supplier wishes to appoint a sub-contractor, the Supplier may appoint such a sub-contractor provided that it has fulfilled all of the following conditions:

9.1.1 the Supplier provides the Customer with full details of the sub-contractor (including the results of the due diligence undertaken in accordance with paragraph 9.1.2) before its appointment and the Customer has consented to such appointment in writing;

9.1.2 the Supplier undertakes thorough due diligence on the proposed sub-contractor, including a risk assessment of the technical and organisational measures implemented by the sub-contractor to meet the requirements of the Data Protection Laws, which shall be used by the Supplier to inform any decision on appointing the proposed sub-contractor;

9.1.3 the sub-contractor contract (as it relates to the protection of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in these Data Processing Terms; and

9.1.4 the sub-contractor's right to Process Personal Data terminates automatically, for whatever reason, on expiry or termination of this Contract or the sub-contract, whichever is earlier.

9.2 The Supplier shall not disclose Personal Data to a third party (including a sub-contractor) in any circumstances unless expressly permitted under these Data Processing Terms or otherwise without the Customer's prior written consent, save in relation to Third Party Requests. For Third Party Requests, the Supplier shall use reasonable endeavours to advise the Customer in advance of such disclosure, unless the Supplier is prohibited by law or regulation from notifying the Customer of that disclosure, in which case it shall do so as soon as practicable thereafter (where permitted by law or regulation).

9.3 Notwithstanding any consent or approval given by the Customer under this paragraph 9, the Supplier shall remain primarily liable to the Customer for the acts, errors and omissions of any such third party and shall be responsible to the Customer for the acts, errors and omissions of such third party as if they were the Supplier's own acts, errors and omissions.

10. DATA RETENTION POLICY

10.1 The Supplier shall not retain Personal Data for longer than is necessary to fulfil the Permitted Purpose, and shall comply with the Customer's prevailing data retention schedules from time to time.

10.2 The Supplier shall (on a request from the Customer) make available to the Customer in electronic form any or all of the Personal Data.

11. INSURANCE

11.1 The Supplier agrees:

11.1.1 to obtain and keep in full force and effect at all times, in respect of the Processing of the Personal Data, a policy or policies of insurance covering liability for damage arising to persons as a result of the Supplier's failure to comply with the GDPR with policy limits and provisions conforming to such requirements as the Customer may from time to time prescribe; and

11.1.2 to deliver to the Customer copies of all applicable insurance policies taken out pursuant to the provisions of this agreement and ensure that the Customer shall be entitled to the benefit of such insurance.

APPENDIX 1

DATA PROCESSOR REQUIREMENTS

1. Accountability and Record keeping

1.1 The Supplier shall, prior to commencing the provision of Services under the Contract, create and maintain detailed records relating to its Processing of Personal Data as will ensure that the Supplier complies with Article 30(2) of the GDPR.

1.2 The aforementioned records shall be in a form which shall be produced to the Customer and/ or the Regulator promptly upon their request.

2. Security Breach Notification

2.1 A written description of the Personal Data Breach Particulars shall be recorded and documented by the Supplier promptly upon occurrence of the same, and shall be provided to the Customer (via its allocated Supplier account manager) along with the notification made by the Supplier under paragraph 3.1.7(g) of these DP Terms.

2.2 In response to each Personal Data Breach the Supplier shall raise a Personal Data Breach support call to its "Projects & Security" team (or equivalent) and the incident will be reported on to the Chief Technology Officer ("**CTO**").

2.3 The Supplier shall empower its CTO to decide if the Personal Data Breach support call requires the formation of an emergency response team to deal with the Personal Data Breach.

2.4 Regardless of whether an emergency response team is created, each Personal Data Breach support call shall result in a root cause analysis being conducted and remediation actions being taken by the Supplier, the details of both to be appropriately documented by the Supplier. In addition, the Supplier shall timeously identify and implement actions to prevent or reduce the probability of the same or a similar Personal Data Breach(s) (re)occurring in the future.

3. Data Protection Officer

3.1 During the Term the Supplier shall have a full time employee appointed in the role of Data Protection Officer. The responsibilities, obligations and right of such employee (the "**DPO**") shall be those identified in the GDPR as being the role and responsibility of the Data Protection Officer (as such term is described in Section 4 of Chapter IV of the GDPR), and shall include:

3.1.1 the development, maintenance and implementation of the Supplier's data protection policy;

3.1.2 the provision of information and guidance on the Processing of all Personal Data to Supplier;

3.1.3 the delivery of training to Supplier staff on the provisions of the GDPR and protection of Personal Data;

3.1.4 the processing, co-ordination and response to all requests for information in respect of Personal Data and or its Processing by the Supplier;

3.1.5 being the nominated officer on the Supplier's data protection register;

3.1.6 ensuring data held by the Supplier remains up-to-date and is destroyed wherever necessary to comply with paragraph 10 of these DP Terms;

3.1.7 advising on all Data Protection Impact Assessments undertaken by the Supplier; and

3.1.8 co-operation and liaison with the Regulator as and when required.

3.2 The Supplier shall ensure that the DPO:

3.2.1 reports to the highest level of management and supervision within the Supplier's organisation;

3.2.2 operates independently of instruction, is freed from conflicts of interest and is not dismissed or penalised for performing its responsibilities;

3.2.3 has the requisite professional qualities and expert knowledge to fulfil its responsibilities;

3.2.4 has sufficient budget and resources available in order to fulfil its responsibilities;

3.2.5 is a permanent member of a business committee where all key decisions regarding business units regarding data protection projects and compliance are taken by the Supplier's business;

3.2.6 shall be involved in all decisions affecting the Supplier's compliance with Data Protection Laws; and

3.2.7 Is involved either directly or indirectly with all projects that involve the collection and Processing of Personal Data.

APPENDIX 2

DATA TRANSFER RISK ASSESSMENT

The following form is to be completed by the Supplier and returned to the Customer where it proposes to make a Data Transfer in accordance with paragraph 5 of these DP Terms:

Description of the Personal Data which will be transferred/ accessed:	
Restricted Country or Countries that the Personal Data will be transferred to or accessed from:	
Description of the means by which the Supplier will ensure the Personal Data is appropriately protected (e.g. Model Clauses):	
Evidence to show that the Supplier has considered the Data Protection Laws in connection with the transfer of the Personal Data to the Restricted Countries noted:	