CALL OFF SCHEDULE 14: ALTERNATIVE AND/OR ADDITIONAL CLAUSES

1. IMPLEMENTATION

1.1 The provisions set out in the following part of this Call Off Schedule 14 (being Alternative and/or Additional Clauses) shall apply to and be deemed to be incorporated into this Call Off Contract. In the event of any conflict or inconsistency between any of these Alternative and/or Additional Clauses and any other provisions of the Call Off Contract, the relevant Alternative and/or Additional Clause shall take priority.

2. GENERAL SCHEME DEFINITIONS

2.1 For the purposes of this Call Off Contract, the following expressions shall have the following meanings:-

2.1.1 "Beneficiary" means a person to whom a Voucher has been issued under and in accordance with the rules of the GHG Scheme;

2.1.2 [redacted]

2.1.3 [redacted]

2.1.4 [redacted]

2.1.5 "GHG Scheme" means the Customer's "Green Homes Grant" scheme, or any similar scheme introduced by the Customer as a replacement for the scheme of that name, for providing grant support in respect of certain energy related building improvement measures, being the scheme which is the subject of the Services;

2.1.6 "GHG Scheme Participant" means any person who has applied for or received or (as the context requires) may wish to apply for a Voucher or who is or (as the context requires) may wish to become an approved installer under the GHG Scheme;

2.1.7 "GHG Scheme Participant Terms and Conditions" means (as the context requires) the terms and conditions for participating in the GHG Scheme between the Supplier and a GHG Scheme Participant;

2.1.8 "Grant Funds" means any monies provided by the Customer to the Supplier for the purpose of putting the Supplier in funds in order to make Grant Payments (being monies which are to be dealt with separately from amounts payable to the Supplier by way of Charges);

2.1.9 "Grant Payment" means any amount payable to a relevant installer on behalf of a Beneficiary by way of the redemption of a Voucher under, and subject to, the rules of the GHG Scheme (including the relevant terms and conditions on which the relevant Voucher was issued);

2.1.10 "ICO" means the Information Commissioner's Officer or any successor supervisory authority as applicable from time to time;

2.1.11 [redacted]

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

2.1.12 [redacted]

2.1.13 [redacted]

2.1.14 [redacted]

2.1.15 [redacted]

2.1.16 "Scheme Affiliate" means a third party organisation or public authority that discloses and/or receives Personal Data, in its capacity as a Data Controller, from the Supplier relating to a GHG Scheme Participant for the purpose of providing additional information or evaluation to assist with or evaluate the delivery of the Services pursuant to the GHG Scheme; and

2.1.17 "Voucher" means a voucher issued under the GHG Scheme by way of an offer of grant support in respect of one or more energy related building improvement measures.

3. CHARGING STRUCTURE & CHARGES

3.1 Subject to paragraph 3.2 of this Call Off Schedule 14, the Charges payable under this Call Off Contract shall [redacted]

3.2 [redacted]

3.2.1 [redacted]

3.2.2 [redacted]

3.3 For the purposes of this Call Off Contract:-

3.3.1 [redacted]

[redacted]

3.3.2 [redacted]

3.3.3 [redacted]

3.3.4 [redacted]

3.4 [redacted]

4. EXIT MANAGEMENT

4.1 On being given any notice of termination under this Call Off Contract, or at any time after any such notice is given (whether by the Customer or the Supplier), the Supplier shall comply with such reasonable instructions as the Customer may provide in respect of the following matters:-

4.1.1 the administration of the GHG Scheme, including (without prejudice to the generality of the Supplier's obligations under paragraph 8 of this Call Off Schedule 14) instructions requiring the Supplier to cease issuing any further Vouchers;

4.1.2 communications in relation to the GHG Scheme, including instructions requiring the Supplier to cease or modify particular communications directed at actual or prospective GHG Scheme Participants;

4.1.3 the return or permanent deletion of any Personal Data processed by the Supplier under the Call Off Contract.

4.2 On being requested to do so from time to time, the Customer shall promptly include in its then current Exit Plan such provision in relation to the matters referred to in paragraph 4.1 of this Call Off Schedule 14 as the Customer may reasonably require.

5. AGREEMENT AND IMPLEMENTATION OF KPIS, SERVICE LEVELS & SERVICE CREDIT REGIME

5.1 [redacted]

5.1.1 [redacted]

5.1.2 [redacted]

5.1.3 [redacted]

5.2 In setting the agreed KPIs, Service Levels and Service Credit regime and the phasing of its implementation, the Parties shall ensure that the measures are reasonable and consistent with supporting the achievement of the objectives of the Green Homes Grant Voucher Scheme as set out in Schedule 2 (Services Description). For that discussion the Parties shall take as a starting point the table of indicative KPI/Service Levels contained in Annex D to the invitation to tender for this Call Off Contract while recognising that this represents only the Customer's current thinking at that time, and was tabled as subject to further consideration by the Parties. [redacted]. If the Parties are unable to agree the KPIs, Service Levels and Service Credit regime [redacted] the Parties will refer the Dispute for resolution in accordance with Schedule 11 (Dispute Resolution Procedure) using the Expedited Dispute Timetable.

6. DATA

6.1 The definition of "*Restricted Countries*" at Call Off Schedule 1: Definitions shall be deleted in its entirety.

6.2 At Clause 34.2.8 of the Call Off Contract, the word *"Supplier"* in the sentence: *"If the Customer Data is corrupted, lost or sufficiently degraded as a result of a Default so as to be unstable, the Supplier may:…"* will be replaced with the word *"Customer"* to read: *"If the Customer Data is corrupted, lost or sufficiently degraded as a result of a Default so as to be unstable, the Customer may:…".*

6.3 Clause 34.6 of the Call Off Contract (Protection of Personal Data) shall be deleted in its entirety and replaced with the Data Protection Appendix attached to this Call Off Schedule 14.

6.4 References to clause 34.6 at clauses 23.1.2; 29.2.3(e)(i); and 45.4.1(b) in the Call Off Contract shall be replaced with the words "*the Data Protection Appendix*".

6.5 The definitions of 'Data Processor' and 'Data Controller' shall be deleted from the Call Off Contract and all references to "*Data Processor*" and "*Data Controller"* in the Call Off Contract shall be amended to "*Processor*" and "*Controller*", respectively.

7. PROSPECTIVE CHANGES TO IN-HOUSE AUDITS

7.1 Subject to compliance with clause 22 (Change) of the Call Off Contract, the Customer shall be entitled at any time to vary the scope of the Services such that some or all of the audit activities to be carried out by the Supplier on an "in house" basis in respect of the GHG

Scheme are removed from the scope of the Services, with a view to the relevant audit activities being carried out by a third party auditor instead and the Supplier interacting with the relevant third party auditor to enable the Supplier to utilise the results of the relevant third party audits in delivering the remainder of the Services. For these purposes, the Supplier shall, if and when requested to do so by the Customer promptly take such steps as may be necessary in order to prepare and agree with the Customer a draft Variation Form and Impact Assessment documenting the basis on which any such variation would be implemented, if required at any time by the Customer.

8. GHG SCHEME PARTICIPANT TERMS AND CONDITIONS AND ISSUE AND REDEMPTION OF VOUCHERS

8.1 The Supplier shall ensure that all GHG Scheme Participant Terms and Conditions between the Supplier and a GHG Participant for taking part in the GHG Scheme shall be in a form as approved by the Customer. The Supplier shall make any changes to the GHG Scheme Participant Terms and Conditions as reasonably required by the Customer during the Call Off Contract Period.

8.2 The Supplier shall ensure that all Vouchers issued under the GHG Scheme are issued subject to and in accordance with such rules and other requirements as the Customer may specify from time to time in reasonable instructions given to the Supplier.

8.3 Without prejudice to the generality of paragraph 8.2 of this Call Off Schedule 14:-

8.3.1 the Supplier shall not commence the issue of any Vouchers until it has Achieved the Milestone M2: Voucher Issuance;

8.3.2 the Supplier shall only issue Vouchers in a manner that is consistent with the eligibility criteria and other rules and requirements applicable to the GHG Scheme, as set by the Customer from time to time;

8.3.3 the Supplier shall promptly comply with any reasonable instruction from the Customer to suspend and/or recommence the issuing and/or redemption of Vouchers; and

8.3.4 the Supplier shall promptly comply with any instructions from the Customer concerning any limit to the number and/or value of Vouchers that can be issued by the Supplier [redacted] as instructed by the Customer.

9. GRANT FUND MONIES

9.1 The Supplier may only use Grant Fund monies to make Grant Payments during the continuation of the GHG Scheme [redacted]

9.1.1 [redacted]

9.1.2 [redacted]

9.2 [redacted]

9.3 The Parties agree, and the Supplier shall ensure that, all Grant Fund monies received by the Supplier from time to time shall be held, pending their use in accordance with paragraph

9.1 of this Call Off Schedule 14, on trust for the Customer in a dedicated bank account which contains no monies other than Grant Fund monies.

9.4 The Supplier shall operate the Grant Fund in accordance with the principles set out in paragraph 6.1.19 of Annex 1 (The Services) to Call Off Schedule 2 (Services) and the Parties shall additionally operate the Grant Fund in accordance with the following agreed principles:

9.4.1 [redacted]

9.4.2 [redacted]

9.4.3 [redacted]

9.4.4 [redacted]

9.4.5 the Supplier shall inform the Customer of the balance of the Grant Fund as soon as practicable upon any request; and

9.4.6 where the Supplier requires an interim replenishment of Grant Fund monies outside of the replenishment schedule envisaged by paragraph 9.4.3 by reason of a more rapid request for valid Grant Payments than anticipated, the Supplier may request an interim payment for additional Grant Fund monies to enable the Supplier to meet the envisaged Grant Payments until the date that the Supplier would next be entitled to request Grant Fund monies in accordance with Paragraph 9.4.3.

9.5 [redacted]

9.6 Any balance of the Grant Fund monies [redacted] held by the Supplier (in so far as they have not already been committed by the Supplier for payment by way of Grant Payments in accordance with the rules of the GHG Scheme) shall be returned to the Customer as soon as reasonably practicable and [redacted] after:

9.6.1 the expiry, termination or any suspension of the Call Off Contract or of the GHG Scheme (if earlier); or

9.6.2 the Customer's reasonable demand (by notice in writing).

9.7 [redacted]

10. COVID-19/ PANDEMIC / EU EXIT AND TRANSITION

10.1 The definition 'Force Majeure' shall be amended so that the definition is titled 'Force Majeure Event" and the definition of 'Affected Party' shall be amended by adding the word 'Event' at the end so that it reads 'means the party seeking to claim relief in respect of a Force Majeure Event'.

10.2 For the purposes of this Call Off Contract (including Clause 40), the Supplier acknowledges and agrees that:-

10.2.1 the actual or potential impacts on the provision of the Services of: (i) COVID-19 or any similar pandemic; and (ii) the United Kingdom's exit and transition from the European Union (including the end of any relevant transition period on a "no deal" basis) are (in both cases) known to the Supplier, and the Supplier has designed the Services to be resilient to such risks; and

10.2.2 accordingly, the occurrence and/or any impacts of any such events (including any associated Change in Law) shall not constitute Force Majeure Events.

11. COMPENSATION [redacted]

11.1 The Supplier acknowledges and agrees that:-

11.1.1 it is required as part of the Services to design a complaints handling process for GHG Scheme Participants that will include the possibility of payment of compensation to a GHG Scheme Participant who has suffered loss as a result of any failure on the part of the Supplier to comply with any obligations owed by it to that GHG Scheme Participant, [redacted]

11.1.2 [redacted]

12. CALL OFF CONTRACT CLAUSE 13.6

12.1 The Parties have agreed that Call Off Contract Clause 13.6 should read as follows:

'13.6 A Service Credit shall be the Customer's exclusive financial remedy for a Service Level Failure except where:

13.6.1 [redacted]

13.6.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier or any Supplier Personnel; or

(c) results in:

(i) the corruption or loss of any Customer Data (in which case the remedies under Clause 34.2.8 (Protection of Customer Data) shall also be available); and/or

(ii) the Customer being required to make a compensation payment to one or more third parties; and/or

13.6.3 the Customer is otherwise entitled to or does terminate this Call Off Contract pursuant to Clause 41 (Customer Termination Rights) except Clause 41.7 (Termination Without Cause).'

13. MODERN SLAVERY

13.1 The Supplier shall, and procure that each of its Sub-Contractors shall, comply with:

13.1.1 the Modern Slavery Act 2015 ("Slavery Act"); and

13.1.2 the Customer's anti-slavery policy as provided to the Supplier from time to time ("Anti-slavery Policy").

13.2 The Supplier shall:

13.2.1 implement due diligence procedures for its Sub-Contractors and other participants in its supply chains, to ensure that there is no slavery or trafficking in its supply chains;

13.2.2 respond promptly to all slavery and trafficking due diligence questionnaires issued to it by the Customer from time to time and shall ensure that its responses to all such questionnaires are complete and accurate;

13.2.3 prepare and deliver to the Customer each year, an annual slavery and trafficking report setting out the steps it has taken to ensure that slavery and trafficking is not taking place in any of its supply chains or in any part of its business;

13.2.4 maintain a complete set of records to trace the supply chain of all Services provided to the Customer regarding the Call Off Contract; and

13.2.5 implement a system of training for its employees to ensure compliance with the Slavery Act.

13.3 The Supplier represents, warrants and undertakes throughout the Call Off Contract Period that:

13.3.1 it conducts its business in a manner consistent with all applicable laws, regulations and codes including the Slavery Act and all analogous legislation in place in any part of the world;

13.3.2 its responses to all slavery and trafficking due diligence questionnaires issued to it by the Customer from time to time are complete and accurate; and

13.3.3 neither the Supplier nor any of its Sub-Contractors, nor any other persons associated with it:

(a) has been convicted of any offence involving slavery and trafficking; or

(b) has been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence regarding slavery and trafficking.

13.4 The Supplier shall notify the Customer as soon as it becomes aware of:

13.4.1 any breach, or potential breach, of the Anti-Slavery Policy; or

13.4.2 any actual or suspected slavery or trafficking in a supply chain which relates to the Contract.

13.5 If the Supplier notifies the Customer pursuant to paragraph 13.4, it shall respond promptly to the Customer's enquiries, co-operate with any investigation, and allow the Customer to audit any books, records and/or any other relevant documentation in accordance with the Contract.

13.6 If the Supplier is in Default under paragraphs 13.2 or 13.3 the Customer may by notice:

13.6.1 require the Supplier to remove from performance of the Call Off Contract any Sub-Contractor, Staff or other persons associated with it whose acts or omissions have caused the Default; or

13.6.2 immediately terminate the Call Off Contract.

14. SUPPLIER PERSONNEL

The Supplier shall ensure that all Services are provided on an independent and impartial basis and in particular (but without limitation) that no actual or potential conflict of interest arises, or could reasonably be perceived as being at risk of arising, between the duties of any Supplier Personnel as a matter of this Call Off Contract when carrying out audits in respect of any particular GHG Scheme Participant and any other interest or relationship (whether personal, commercial or otherwise) the relevant Supplier Personnel may have in or with the relevant GHG Scheme Participant.

15. TRANSPARENCY REPORTS

15.1 Within 20 Working Days of the Call Off Commencement Date the Parties shall work together to agree, and formalise by way of a Variation the List of Transparency Reports to be inserted into Annex A (List of Transparency Reports) of Call Off Schedule 13 (Transparency Reports).

15.2 If the Parties are unable to agree the List of Transparency Reports [redacted] the Parties will refer the Dispute for resolution in accordance with Schedule 11 (Dispute Resolution Procedure) using the Expedited Dispute Timetable.

16. TESTING

16.1 Pursuant to paragraphs 3 (Test Strategy) and 4 (Test Plans) of Call Off Schedule 5 (Testing), the Parties agree that by [redacted] the Supplier will deliver:

16.1.1 the draft Test Strategy for approval by the Customer; and

16.1.2 draft Test Plans for approval by the Customer.

16.2 For the avoidance of doubt, paragraph 4.3 of Call Off Schedule 5 (Testing) shall also apply to the approval by the Customer of the draft Test Strategy such that the Customer may not also unreasonably withhold or delay its approval of the draft Test Strategy. The Parties plan to be able to agree the Test Strategy and Test Plans [redacted]

16.3 [redacted]

16.3.1 [redacted]

(a) [redacted]

(b) [redacted]

(c) [redacted]

16.3.2 [redacted]

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

(f) [redacted]

(g) [redacted]

(h) [redacted]

(i) [redacted]

(j) [redacted]

(k) [redacted]

(l) [redacted]

(m) [redacted]

(n) [redacted]

(o) [redacted]

16.4 [redacted]

[redacted]

17.1 [redacted]

17.1.1 [redacted]

17.1.2 [redacted]

17.2 [redacted]

[redacted]

18.1 [redacted]

18.2 [redacted]

19. [redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

		[redacted]		
[redacted]		[redacted]		
[redacted]		[redacted]		
[redacted]		[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]
24	[redacted]	[redacted]	[redacted]	[redacted]
25	[redacted]	[redacted]		
26	[redacted]	[redacted]	[redacted]	[redacted]
27	[redacted]	[redacted]	[redacted]	[redacted]
28	[redacted]	[redacted]	[redacted]	[redacted]
29	[redacted]	[redacted]	[redacted]	[redacted]
30	[redacted]	[redacted]	[redacted]	[redacted]
31	[redacted]	[redacted]	[redacted]	[redacted]
32	[redacted]	[redacted]	[redacted]	[redacted]
33	[redacted]	[redacted]	[redacted]	[redacted]

34	[redacted]	[redacted]		
35	[redacted]	[redacted]	[redacted]	[redacted]
36	[redacted]	[redacted]	[redacted]	[redacted]
37	[redacted]	[redacted]	[redacted]	[redacted]
38	[redacted]	[redacted]		
	[redacted]	[redacted]	[redacted]	
39	[redacted]	[redacted]	[redacted]	[redacted]
40	[redacted]	[redacted]	[redacted]	[redacted]
41	[redacted]	[redacted]	[redacted]	[redacted]
42	[redacted]	[redacted]	[redacted]	[redacted]
43	[redacted]	[redacted]	[redacted]	[redacted]
44	[redacted]	[redacted]		
45	[redacted]	[redacted]	[redacted]	[redacted]
46	[redacted]	[redacted]	[redacted]	[redacted]
47	[redacted]	[redacted]	[redacted]	[redacted]
48	[redacted]	[redacted]	[redacted]	[redacted]

		[redacted]		
49	[redacted]	[redacted]	[redacted]	[redacted]
50	[redacted]	[redacted]	[redacted]	[redacted]
51	[redacted]	[redacted]	[redacted]	[redacted]
52	[redacted]	[redacted]	[redacted]	[redacted]
53	[redacted]	[redacted]	[redacted]	[redacted]
54	[redacted]	[redacted]		
55	[redacted]	[redacted]	[redacted]	[redacted]
56	[redacted]	[redacted]	[redacted]	[redacted]
57	[redacted]	[redacted]	[redacted]	[redacted]
58	[redacted]	[redacted]	[redacted]	[redacted]
59	[redacted]	[redacted]	[redacted]	[redacted]
60	[redacted]	[redacted]	[redacted]	[redacted]

61	[redacted]	[redacted]	[redacted]	[redacted]
62	[redacted]	[redacted]	[redacted]	[redacted]
63	[redacted]	[redacted]	[redacted]	[redacted]
64	[redacted]	[redacted]	[redacted]	[redacted]
65	[redacted]	[redacted]	[redacted]	[redacted]
66	[redacted]	[redacted]	[redacted]	[redacted]
67	[redacted]	[redacted]		
	[redacted]	[redacted]	[redacted]	

[redacted]

DATA PROTECTION APPENDIX

1. Data Protection Appendix

1.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer will act as the Controller and the Supplier may act as Processor, or as a joint Controller, depending on the purposes for processing agreed between the parties. The processing that the Supplier is authorised by the Customer to do as Processor is listed in Annex 1 to this Schedule (Processing Personal Data as Processor) and may not be determined by the Supplier. The processing that the Supplier is authorised by the Customer to do as Controller is listed in Annex 2 to this Schedule (Processing Personal Data as Controller) and may be determined by the Customer jointly with the Supplier.

1.2. The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

1.3. The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4. The Supplier shall implement all appropriate technical and organisational measures to ensure a level of security appropriate to protect the Personal Data it processes under this Call Off Contract in compliance with the Data Protection Legislation.

1.5. The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Call Off Contract:

(a) process that Personal Data only in accordance with Annex 1 (Processing Personal Data as Processor) or Annex 2 (Processing Personal Data as Controller), as applicable in the circumstances, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Supplier Personnel do not process Personal Data except in accordance with this Data Protection Appendix (and in particular Annex 1 (Processing Personal Data as Processor) or Annex 2 (Processing Personal Data as Controller) (as applicable);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Supplier's duties under this Data Protection Appendix;

(B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Call Off Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) subject to paragraph 1.5(f), not transfer Personal Data outside of the UK or the EU unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

(i) the Customer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and

(iv) the Supplier complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Call Off Contract unless the Supplier is required by Law to retain the Personal Data;

(f) the Customer consents to the processing of Personal Data by the Supplier in the United States of America for the duration of the Call Off Contract Period, provided always that:

(i) prior to the commencement of such processing, the Supplier enters into the European Commission's standard contractual clauses applicable to data exports from the EU (and the UK) to a third country;

(ii) on or before 30 September 2020 the Supplier shall implement an intra-group data transfer agreement which includes as a minimum:

(A) the standard contractual clauses referenced in paragraph 1.5(f)(i) above;

(B) such additional protections which the Supplier, acting reasonably, identifies as being required to ensure that personal data relating to

UK and EU data subjects which is processed in the United States of America is afforded equivalent protection to that being processed in the UK;

(C) confirmation as to why public authorities in the United States of America would not have the same access rights, or (if they do have those rights) be likely to exercise them, as they would in respect of providers of electronic communications services as defined for the purposes of U.S. law in 50 U.S.C. § 1881(b)(4) (FISA Act Amendments);

(D) an obligation on the Supplier to ensure a flow-down of substantially the same provisions and protections as are contained within the intra-group data transfer agreement to any Processors/Sub-processors; and

(E) an obligation on the Supplier to review and update as necessary the intra-group data transfer agreement promptly following any new mandatory guidance or standard clauses being issued by the UK Government, ICO or other applicable regulator.

For the avoidance of doubt, the Customer does not have the right to approve or reject the terms of the Supplier's intra-group data transfer agreement, provided that points (A) to (E) above are included within that agreement;

(iii) the Supplier shall:

(A) notify the Customer without delay of any legally binding request by any U.S. law enforcement authority for disclosure of the UK Personal Data; and

(B) take legal action against any disclosure of such Personal Data and refrain from disclosing Personal Data to the relevant authorities until a competent court of last resort has ordered the Supplier to disclose the Personal Data; and

(iv) the Supplier shall provide [redacted] assistance to the Customer in the completion of a data transfer assessment in the form set out at Annex 4. The Parties shall use [redacted] to complete the data transfer assessment [redacted]

1.6. The Supplier shall notify the Customer [redacted] if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the ICO or any other regulatory Customer in connection with Personal Data processed under this Call Off Contract;

(e) receives a 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

(f) becomes aware of a Data Loss Event.

1.7. The Supplier's obligation to notify under paragraph 1.6 shall include the provision of further information to the Customer in phases, as details become available.

1.8. Taking into account the nature of the processing, the Supplier shall provide the Customer with [redacted] in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made to either the Supplier or the Customer by any Data Subject in relation to Personal Data processed under this Call Off Contract (and insofar as possible within the timescales reasonably required by the Customer) including by [redacted] providing:

(a) the Customer with full details and copies of the complaint, communication or request;

(b) such assistance as is [redacted] requested by the Customer to enable the Customer to comply with the request within the relevant timescales set out in the Data Protection Legislation;

(c) the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Customer following any Data Loss Event;

(e) assistance as requested by the Customer with respect to any request from the ICO, or any consultation by the Customer with the ICO;

(f) non-automated verification of any automated decision making where the Data Subject of the decision requests for that automated decision to be verified.

1.9. The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Data Protection Appendix. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

(a) the Customer determines that the processing is not occasional;

(b) the Customer determines the processing includes special category personal data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.10. The Supplier shall allow for audits of its Personal Data Processing activity by the Customer or the Customer's designated auditor.

1.11. The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.12. Before allowing any Sub-processor to process any Personal Data related to this Call Off Contractthe Supplier must:

(a) notify the Customer in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Customer;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Data Protection Appendix such that they apply to the Sub-processor; and

(d) provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require.

1.13. The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.14. The Supplier undertakes to enter into a data processing agreement with any Scheme Affiliate who, acting in its capacity as a Controller, will be Processing and/or receiving or accessing Personal Data from the Supplier (acting in its capacity as a Processor) on terms which are substantially the same as those agreed between the Customer and the Supplier relating to the processing of Personal Data. Without limitation, as at the Call Off Commencement Date, it is envisaged that data processing agreements will be required to be entered by the Supplier with the following Scheme Affiliates:

[redacted]

1.15. The Supplier may, at any time on [redacted] notice, revise this Data Protection Appendix by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Call Off Contract).

1.16. The Parties agree to take account of any guidance issued by the ICO. The Customer may on [redacted] notice to the Supplier amend the Call Off Contract to ensure that it complies with any guidance issued by the ICO.

1.17. The Customer may at any time on not less than 30 Working Days' notice (or such shorter period as is required by Law), revise this Data Protection Appendix to reflect the introduction of or amendment to any Law (including mandatory guidance or codes of practice issued by the UK Government, the ICO or the European Data Protection Board) which implements or requires the implementation of additional or alternative appropriate safeguards for the transfer of Personal Data from the UK to the United States of America, following the judgment of the Court of Justice of the European Union in Case C-311/18 1.16.1.18. (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems). Where any such revisions are requested, they shall be progressed as a Specific Change in Law.

Annex 1 - Processing Personal Data as Processor

1. The contact details of the Customer Data Protection Officer are:

[redacted]

[redacted]

[redacted]

2. The contract details of the Supplier Data Protection Officer are:

[redacted]

[redacted]

[redacted]

3. The Processor shall comply with any further written instructions with respect to processing by the Controller.

4. Any such further instructions shall be incorporated into this Annex.

Contract Reference:	
Date:	
Description Of Authorised Processing	**Details**
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor in accordance with paragraph 1.1. of the Data Protection Appendix.
Subject matter of the processing	Of the activities being conducted under the Call Off Contract, the Supplier shall act as Processor for the following: • Evaluation • When processing any information where the applicant has been in receipt of assistance via other government grant schemes (e.g. ECO, RHI, GHG LAD, Green Deal etc.). The subject matter of the processing is to enable the Supplier to provide the Services described in the Call Off Contract. In relation to applicants, the purpose is for the assessment of access to, and redemption of, the Green Homes Grant Voucher Scheme.

Duration of the processing	The data will be kept for the duration of the scheme, plus as long as is necessary for monitoring and evaluation, and thereafter following final closure of the Green Homes Grant Voucher Scheme in accordance with the Data Retention Policy from time to time in force.
Nature and purposes of the processing	The nature of the processing includes the collection, recording, organisation, structuring, storage, adaptation or alteration (where necessary), retrieval, consultation, use, sharing, erasure and destruction of data. The purpose of the processing is the delivery of the Green Homes Grant Voucher Scheme.
Type of Personal Data	• The personal data relates to the delivery of the main scheme and may comprise the following types of personal data: **Personal Data** • Name of data subject • Contact details including address, telephone number and email address • Summary of eligibility criteria including benefit information • Home-ownership/tenure status and related information • Information where the applicant has been in receipt of assistance via other government grant schemes (e.g. ECO, RHI, GHG LAD, Green Deal etc.) • Customer account data **Special category personal data** • The nine protected characteristics set out under the public sector equality duty: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation • Health conditions • Ethnicity • Gender **Other information which does not constitute personal data but may be processed** • Size and composition of household • Number of children or older household members (if any) • Annual income • Receipt of benefits • Education level • Whether long-standing limiting illness in household • Customer referral source • Customer source for initial awareness
Categories of Data Subject	• Staff (including volunteers, agents, and temporary workers) • Applicants and other household members • Installers • Users of the website

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Data to be returned or destroyed in accordance with the provisions of the Call Off Contract

Annex 2 - Processing Personal Data as Controller

1. The contact details of the Customer Data Protection Officer are:

[redacted]

[redacted]

[redacted]

5. The contract details of the Supplier Data Protection Officer are:

[redacted]

[redacted]

[redacted]

2. Under the circumstances described in the table below, the Customer and the Supplier shall jointly act as Controllers of the Personal Data and further written instructions with respect to processing undertaken by the Supplier when acting as a Controller will be provided by the Customer.

3. Any such further instructions shall be incorporated into this Annex 2.

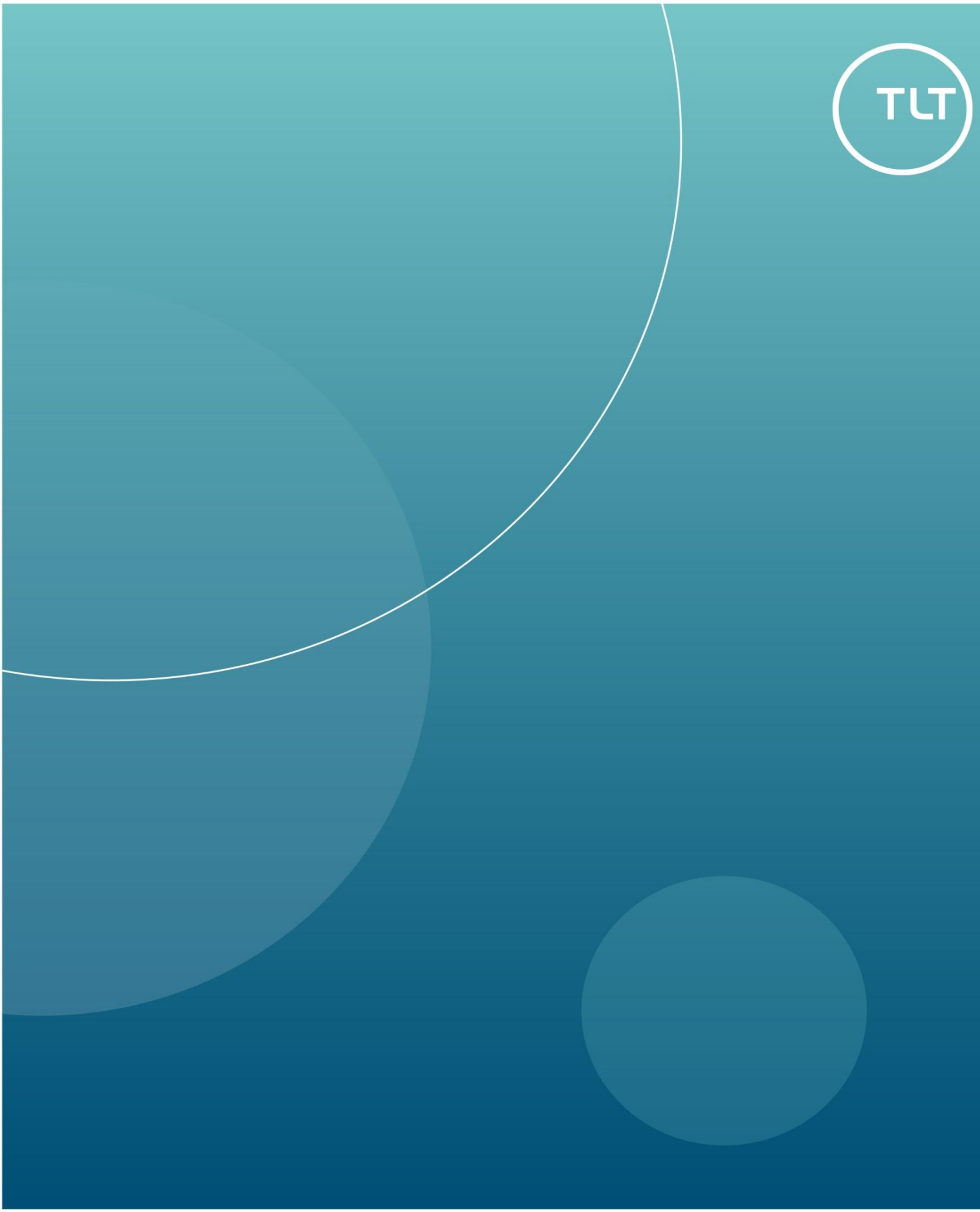
Contract Reference:	
Date:	
Description Of Authorised Processing	**Details**
Identity of the Controller and Processor	The Parties acknowledge that they are joint Controllers for the purposes of the Data Protection Legislation in respect of the Personal Data which the purposes and means of the processing is determined by the both Parties as detailed in this Annex 2.
Subject matter of the processing	Of the activities being conducted under the Call Off Contract, the Customer and the Supplier shall act as joint Controllers for the following: • Scheme delivery • Monitoring • Post-payment audits The subject matter of the processing is to enable the Supplier to provide the Services described in the Call Off Contract. In relation to applicants, the purpose is for the assessment of access to, and redemption of, the Green Homes Grant Voucher Scheme.

Duration of the processing	The data will be kept for the duration of the scheme, plus as long as is necessary for monitoring and evaluation, and thereafter following final closure of the Green Homes Grant Voucher Scheme in accordance with the Data Retention Policy from time to time in force.
Nature and purposes of the processing	The nature of the processing includes the collection, recording, organisation, structuring, storage, adaptation or alteration (where necessary), retrieval, consultation, use, sharing, erasure and destruction of data. The purpose of the processing is the delivery of the Green Homes Grant Voucher Scheme.
Type of Personal Data	The personal data relates to the delivery of the main scheme and may comprise the following types of personal data: **Personal Data** • Name of data subject • Contact details including address, telephone number and email address • Summary of eligibility criteria including benefit information • Home-ownership/tenure status and related information • Information where the applicant has been in receipt of assistance via other government grant schemes (e.g. ECO, RHI, GHG LAD, Green Deal etc.) • Customer account data **Special category personal data** • The nine protected characteristics set out under the public sector equality duty: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation • Health conditions • Ethnicity • Gender **Other information which does not constitute personal data but may be processed** • Size and composition of household • Number of children or older household members (if any) • Annual income • Receipt of benefits • Education level • Whether long-standing limiting illness in household • Customer referral source • Customer source for initial awareness

Categories of Data Subject	• Staff (including volunteers, agents, and temporary workers) • Applicants and other household members • Installers • Users of the website
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Data to be returned or destroyed in accordance with the provisions of the Call Off Contract

Annex 3 – Not Used

Annex 4 –Data Transfer Assessment



Department for Business, Energy and Industrial Strategy - Data transfer assessment

Green Homes Grant Scheme

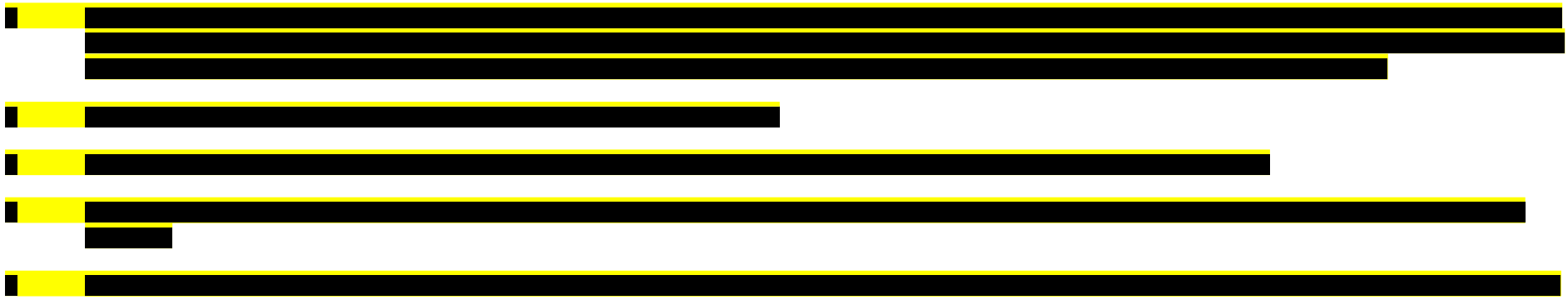
Contents

Department for Business, Energy and Industrial Strategy - Data transfer assessment

Whenever the Department for Business, Energy and Industrial Strategy (**BEIS**) transfers personal data outside the UK or the EEA, it is required to implement appropriate safeguards to ensure that the personal data is protected in the same way as it would be within the UK and the EEA. If BEIS intends to rely on European Commission-approved standard contractual clauses (**SCCs**), then since the Schrems II judgment on 16 July 2020, BEIS is required to conduct an assessment of the recipient country's data protection laws to ensure that they are adequate and do not impinge on the protections provided by the SCCs.

This Data Transfer Assessment (**DTA**) must be completed for any transfers of personal data to a country outside the UK and the EEA (with the exception of the countries listed here) (**third country**), where it is intended that SCCs will be entered into with the recipient.

Please make sure that you:



Section 1: Project details

Project name	*[Insert]*
Recipient details	*[Insert – this should be the recipient entity's full name]*
Third country	*[Insert]*
Project details	*[Guidance: Please include as much information as possible about the project and our relationship with the recipient.]*
Details of data processing carried out by recipient	*[Guidance: Please give as much detail as possible about what the recipient will do with the data transferred. For example, hosting the data; accessing the data remotely for support purposes; transferring data to overseas servers for failover purposes.]*
Purposes of the transfer	*[Guidance: Please describe why the transfer is taking place and why it is necessary, including why it is not possible to keep the data within the UK or EEA.]*
Categories of personal data transferred	*[Guidance: Please list all types of personal data that will be transferred to the recipient, e.g. name, email address, telephone number, gender, marital status, race, salary, bank details etc. If it is not possible to list all types of personal data, for example because the recipient is a cloud storage provider and the categories will depend on the documents/data uploaded, please explain this and give as much information as possible about what data might be transferred.]*
Is there any special category personal data and/or criminal conviction/offence data processed?	*[Guidance: Special category personal data is any data about racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life; sexual orientation; and genetic data or biometric data used to uniquely identify someone. Criminal conviction/offence data includes data about alleged criminal offences as well as about convictions. Please state whether any of this type of data is processed (yes/no) and give details of the particular categories concerned.]*

Categories of data subject	*[Guidance: Please list all categories of individual to whom personal data transferred to the recipient relates, e.g. customers, employees, members of the public. If it is not possible to list all categories of data subject, please explain this and give as much information as you can.]*
Intended duration of the processing	*[Guidance: Please set out how long it is envisaged the recipient will process the data for.]*

Section 2: Transfer assessment

This section is intended to set out the details of the third country's data protection framework and the laws applicable. It is designed to address all of the key principles of the GDPR and assess whether the third country offers an essentially equivalent level of protection in respect of each of those principles.

The Response column should include as much detail as possible about the applicable laws and rules; simple "yes" or "no" answers should be avoided where possible.

The Risk column should set out:

- the risk level of the third country's laws in relation to each specific question, without taking into account any mitigating measures or considerations particular to the project (this will be taken into account in Section 3); and
- the overall risk for each principle where indicated, factoring in the risk level attributed to each question relating to that principle.

Question	Response	Risk
Part 1: Basic Concepts	**Overall risk for principle:**	**H/M/L**
What laws and/or rules are in place (**data protection rules**) governing the collection and use of personal data?	*[Guidance: Please set out as much detail as possible about the legal framework governing data protection in the third country.]*	H/M/L
Are there any additional rules or laws that are pending implementation?	*[Guidance: This should include both: a) any planned reforms of data protection laws, with information about their status and intended timeframe for implementation; and b) if relevant, whether the third country has missed any deadlines for implementation of legislation that the third country was required to implement.]*	H/M/L
Has the country previously applied for a European Commission adequacy decision and been unsuccessful?	*[Guidance: Please also include details of when the adequacy application was made, the reasons for rejection and any changes that have been made to the third country's data protection rules/framework since then.]*	H/M/L

Question	Response	Risk
To whom do the data protection rules apply? Are there any exemptions/specific requirements for particular types of organisations, such as public authorities or law enforcement/national security/defence agencies?	*[Guidance: Please set out all types of organisations that are subject to the data protection rules (i.e. the equivalent to the GDPR concepts of "controller" and "processor") and whether there are different rules for particular types of organisations. For example, in the UK, law enforcement bodies are subject to a different regime when they process personal data for law enforcement purposes.]*	H/M/L
Who is protected by the data protection rules? Are any persons (e.g. children or vulnerable people) treated differently, and if so, how?	*[Guidance: Please include details of who the "data subjects" are for the purposes of the third country's data protection rules and any sub-categories of data subjects to whom the rules apply differently. For example, in the UK there are additional rules that apply to processing of children's data.]*	H/M/L
What types of data do the data protection rules cover? Are any types of personal data treated differently, and if so, how?	*[Guidance: Please set out how the third country defines the concept of "personal data" and whether there are sub-categories of this that are treated differently, and if so how brief details of how they are treated differently. For example, under the GDPR, special categories of personal data and criminal conviction data are treated differently in that they require an additional processing condition/authorisation to be in place to process the data.]*	H/M/L
What types of processing do the data protection rules cover? Are any types of processing treated differently, and if so, how?	*[Guidance: Please set out how the third country defines the concept of "processing".]*	H/M/L
Part 2: Transparent, lawful and fair processing	**Overall risk for principle:**	**H/M/L**
Do the data protection rules require particular lawful grounds or justifications to be in place to process personal data? Are there any exemptions or specific requirements regarding data processing for law enforcement, national security and/or defence purposes?	*[Guidance: Please refer to the specific requirements of the data protection rules regarding lawful basis for processing. For example, if answering this for a country subject to the GDPR, the answer would refer to Article 6 and list the potential lawful bases.]*	H/M/L
Do the data protection rules impose obligations on organisations to inform individuals how their data will be processed? Are there any exemptions or	*[Guidance: Articles 13 and 14 of the GDPR require certain information to be provided to individuals about how their personal data is processed. Please set out details of any similar requirements and what information is required to be provided.*	H/M/L

Question	Response	Risk
specific requirements regarding data processing for law enforcement, national security and/or defence purposes?	*Please also detail whether there are requirements as to the form and format of the information and the point at which it must be provided. Set out any exemptions or specific requirements for particular organisations/processing types.]*	
Part 3: Purpose limitation	**Overall risk for principle:**	**H/M/L**
Do the data protection rules place any restrictions on using personal data for purposes other than those for which the personal data was originally collected? Are there any exemptions or specific requirements regarding data processing for law enforcement, national security and/or defence purposes?	*[Guidance: Please include details of any purpose limitation obligations and how these differ for particular organisations, if at all. For example, under the GDPR, controllers must ensure that personal data is processed for specified and legitimate purposes and only processed for further, incompatible purposes with consent.]*	H/M/L
Part 4: Data quality and proportionality	**Overall risk for principle:**	**H/M/L**
What obligations do the data protection rules impose on organisations to ensure personal data is kept accurate and up-to-date?	*[Guidance: The GDPR requires controllers to ensure personal data is accurate and take reasonable steps to keep it up-to-date. Please detail any equivalent or similar obligations, if they exist.]*	H/M/L
Do the data protection rules contain controls in relation to how much personal data can be processed?	*[Guidance: This refers to the GDPR concept of data minimisation, which means personal data must be limited to only what is necessary for the purposes of processing. Please include details of any similar obligations in the third country's data protection rules.]*	H/M/L
Part 5: Data retention	**Overall risk for principle:**	**H/M/L**
Do the data protection rules contain controls in relation to how long personal data can be stored and/or processed for?	*[Guidance: The GDPR requires personal data to be retained for no longer than necessary for the particular purposes of processing. Please set out any similar rules.]*	H/M/L
Part 6: Security and confidentiality	**Overall risk for principle:**	**H/M/L**

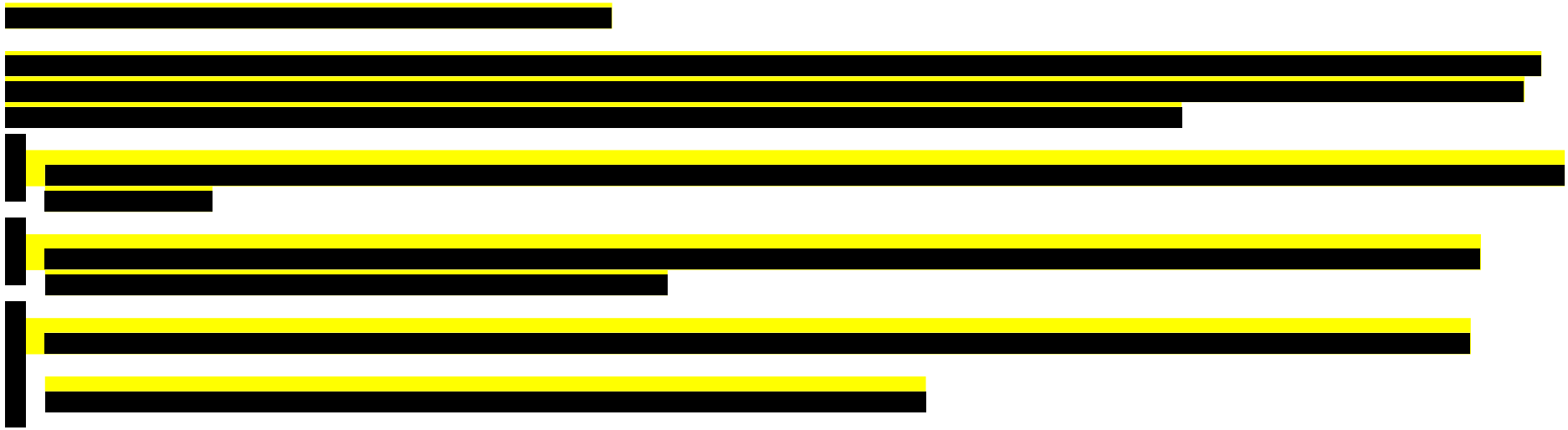
Question	Response	Risk
Do the data protection rules impose security requirements to protect against risk such as accidental disclosure of personal data?	*[Guidance: Please set out any obligations that are imposed on organisations to keep personal data secure, including whether there are any particular security measures referred to (such as pseudonymisation or encryption).]*	H/M/L
What processes must take place in the event of a security breach or other breach of data protection rules?	*[Guidance: Include details of what organisations are required to do in the event of a personal data breach, for example notifying regulators, affected individuals and/or other organisation (e.g. whether data processors have to notify data controllers). Please include details about any timescales imposed for notification and any information that the rules mandate have to be included in any notifications.]*	H/M/L
Part 7: Data subject rights	**Overall risk for principle:**	**H/M/L**
Do the data protection rules provide individuals with any rights over their personal data? If so, what are these rights? Are there any limitations on these rights?	*[Guidance: The GDPR sets out a number of rights that data subjects have over their personal data, e.g. right of subject access, right to erasure, right to rectification, right to object etc. Please set out details of any rights that the third country's data protection laws grant and whether there are any limitations/exemptions that apply to those rights.]*	H/M/L
Part 8: Onward transfers	**Overall risk for principle:**	**H/M/L**
Do the data protection rules place restrictions and obligation on onward transfers of personal data outside the third country?	*[Guidance: This answer should include details of whether organisations in the third country are required to comply with particular requirements when they transfer personal data to another third country. This is a very important aspect of this DTA, as it is crucial that even if we determine we can transfer personal data to the immediate recipient, we understand the implications of any potential onward transfers of that personal data.]*	H/M/L
Can personal data be transferred freely (i.e. without any further safeguards) to any specified countries, territories or sectors or international organisations? If so, on what grounds are these	*[Guidance: This question is aimed at understanding whether, if the third country does impose restrictions on overseas transfers, there are any countries to which the third country allows unfettered transfers without taking any additional steps. This would be the equivalent for the UK and the EEA of the European Commission/UK government adequacy decisions.]*	H/M/L

Question	Response	Risk
countries chosen and how does the assessment process work?		
When data is not permitted to be transferred freely, what additional safeguards are specified for transfers to other countries, sectors etc.?	*[Guidance: For countries to which the third country does not allow free transfer of personal data, please set out details of any other safeguards that are specified in the data protection rules (e.g. for the UK and the EEA, this would refer to SCCs, binding corporate rules and derogations.)*	H/M/L
Part 9: Direct marketing	**Overall risk for principle:**	**H/M/L**
Do the data protection rules impose specific requirements on organisations when processing personal data for direct marketing purposes?	*[Guidance: Please set out details of any consent requirements for direct marketing and when those consent requirements apply, including obligations to offer opt-out options and whether there are any exemptions. Please also specify whether the rules apply differently to different types of marketing (e.g. post, email, telephone, text) and/or to different types of recipients of marketing (e.g. consumer marketing vs business marketing).*	H/M/L
Part 10: Surveillance/access by public authorities	**Overall risk for principle:**	**H/M/L**
Are organisations required to provide personal data to public authorities for purposes such as surveillance, law enforcement and national security? What protections and processes are there around such access?	*[Guidance: This is another key element of this DTA. It is very important that we understand any requirements that the third country's government imposes on organisations to hand over personal data to government bodies and the circumstances in which those requirements apply. Please include details of any limitations on those requirements and safeguards placed around access to data.]*	H/M/L
Part 11: Accountability	**Overall risk for principle:**	**H/M/L**
Are there requirements under the data protection rules to build privacy by design into products/solutions?	*[Guidance: Please set out details of any specific obligations to take data protection considerations into account when building products/services/solutions. For example, the GDPR requires organisations to implement data protection principles into processing at the point at which the decision to process personal data is made.]*	H/M/L

Question	Response	Risk
Are there mandatory requirements to carry out data protection impact assessments or other types of risk assessment when carrying out high risk processing?	*[Guidance: Please set out details of any obligations to conduct any types of impact or risk assessments relating to the processing of personal data.]*	H/M/L
Part 12: Regulation and enforcement	**Overall risk for principle:**	**H/M/L**
Do the data protection rules specify penalties or sanctions for failure to protection personal data/failure to comply with the requirements of the data protection rules?	*[Guidance: Please set out what penalties and sanctions organisations are subject to if they breach data protection rules, for example any fines, enforcement notices/undertakings, compensation claims etc.]*	H/M/L
Which body or bodies regulate and enforce the data protection rules? To what extent are those bodies independent from the government?	*[Guidance: Please include details of the relevant regulators (the equivalent to the ICO in the UK, as well as any other regulators that might be relevant, such as financial services regulators) and those regulators' independence from the government in the third country.]*	H/M/L
What powers and responsibilities do regulators have to enforce data protection legislation? What resources do they have and how are they funded?	*[Guidance: The GDPR and the DPA 2018 in the UK grant powers to the ICO to investigate and audit organisations and impose fines/take other enforcement action. Please detail any similar powers and responsibilities for the third country's regulator(s) and set out how the regulator(s) are funded. If there are concerns about the resource available to the regulator(s) to enforce the legislation, please set these out here.]*	H/M/L
Do regulators issue specific guidelines or recommendations in relation to data processing/compliance with the data protection rules?	*[Guidance: The ICO and European regulators issue guidance on a number of areas of data protection compliance. Please confirm whether the third country's regulator(s) also do this and how often guidance is released/updated.]*	H/M/L
What evidence is there that breaches of data protection rules are appropriately enforced?	*[Guidance: This should refer to enforcement action taken in respect of breaches, if any, or confirm if no enforcement action has been taken. For example, if fines/enforcement notices are regularly issued in response to breaches/regulatory investigations, please set this out.]*	H/M/L

Question	Response	Risk
Part 13: Redress for data subjects	**Overall risk for principle:**	**H/M/L**
How can individuals seek redress for infringement of their data protection rights or breach of the data protection rules? Are there any limitations on these rights, in particular for individuals who are not citizens of the third country?	*[Guidance: Please set out details of whether individuals have rights to seek compensation from organisations that put their personal data at risk and what the requirements are to demonstrate the entitlement to compensation (e.g. under the GDPR, individuals have to demonstrate they have suffered damage or distress. You should also include principles from any case law, for example if individuals are able to seek "loss of control" damages without showing distress. It is also important to understand whether UK citizens are able to seek redress in the same way as third country citizens.]*	H/M/L
What evidence is there that individuals are able effectively to get redress for breaches or infringements of their rights, either with regulators, the courts or other administrative bodies?	*[Guidance: Please explain whether there are extensive examples of data subjects successfully obtaining compensation or other redress for breaches of their data protection rights, for example are there lots of examples of cases where this has happened, or is it difficult in practice for individuals to obtain redress?]*	H/M/L
Part 14: Additional information	**Overall risk for principle:**	**H/M/L**
Do the data protection rules apply differently to any foreign nationals, citizens or residents, if not covered above?	*[Guidance: It is important to understand whether UK/EU citizens' data will be protected in the same way as data of citizens of the third country. Therefore, please set out details of any differences in data protection rules where data subjects are foreign nationals, citizens or residents.]*	H/M/L
Are there any exemptions to data protection rules that are not covered above?	*[Guidance: Ideally, any exemptions will have been drawn out above, but please describe whether there are any other exemptions that have not already been covered.]*	H/M/L
Are there any other concerns about the effectiveness of enforcement that are not covered above?	*[Guidance: This should refer to, for example, any perceptions that local regulators are weak/underfunded/ineffective when it comes to enforcement, as well as any local customers and cultures that might put personal data at risk in practice.]*	H/M/L

Section 3: Project risk assessment



Principle	Overall risk identified (H/M/L)	Additional measures/safeguards and other comments	Residual risk after implementing additional measures/safeguards (H/M/L)
	Guidance: Set out overall risk identified for relevant principle in Section 2 above.	*Guidance: This column should include:* ■ *details of any additional safeguards that can be put in place to mitigate the risks, such as anonymisation of the data or encryption (if the risk in column two is **low**, additional safeguards may not be needed but this should still be considered and recorded); and* ■ *any project-specific considerations that will reduce the risk. For example, if the assessment at Section 2 has identified that the third country imposes no transparency obligations on organisations when processing personal data, but in the context of the project this does not pose a risk for [redacted] or for data subjects because the recipient is a supplier/processor and [redacted] is responsible for informing data subjects about the processing, this would reduce the risk.*	*Guidance: Set out the risk level that remains after taking into account the additional measures/safeguards and comments in column three.*
Part 1: Basic concepts			
Part 2: Transparent, fair and lawful processing			
Part 3: Purpose limitation			
Part 4: Data quality and proportionality			
Part 5: Data retention			

Part 6: Security and confidentiality
Part 7: Data subject rights
Part 8: Onward transfers
Part 9: Direct marketing
Part 10: Surveillance/access by public authorities
Part 11: Accountability
Part 12: Regulation and enforcement
Part 13: Redress for data subjects
Part 14: Additional information

Section 4: Sign off and record outcomes

To be completed by client's DPO in conjunction with project lead.

Item	Comments	Name/position	Date
Advice and decision on transfer, risk and acceptability of SCCs:			
Recommended actions/next steps:			
Data protection advice accepted or overruled:			
Consultation with/notification to ICO required?			

Final sign off and review dates			
Signed:	Name:	Position:	Date:
Next review date			

tltsolicitors.com/contact

Belfast | Bristol | Edinburgh | Glasgow | London | Manchester | Piraeus