

Agreement for Accreditation Services

This Agreement is dated

14 November 2022

Between:

- (1) **The Information Commissioner**, a corporation sole continuing under the Data Protection Legislation, whose main office is at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF (the "**Commissioner**"); and
- (2) **The United Kingdom Accreditation Service** a company limited by guarantee incorporated in England and Wales under no. 3076190 and having its registered office at 2 Pine Trees, Chertsey Lane, Staines-upon-Thames, Surrey TW18 3HR ("**UKAS**").

Background:

The Commissioner:

- A. The Commissioner is a corporation sole appointed by Her Majesty the Queen to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.
- B. The Commissioner is responsible for monitoring and enforcing the provisions of the United Kingdom General Data Protection Regulation and the Data Protection Act 2018.

UKAS:

- C. UKAS is appointed as the national accreditation body by Accreditation Regulations 2009 (SI No 3155/2009) and The Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019 UK Statutory Instruments 2019 No. 696 (as amended). UKAS operates under a Memorandum of Understanding with the Government, through the Secretary of State for Department for Business, Energy & Industrial Strategy. UKAS is a non-profit-distributing private company, limited by guarantee and is independent of Government. It is recognised by government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services.

Certification procedures under the UK GDPR:

- D. Article 42.1 of the UK GDPR sets out that the Commissioner shall encourage the establishment of data protection Certification mechanisms, for the purpose of demonstrating compliance with the UK GDPR by controllers and processors.

- E. Article 42.5 of the UK GDPR sets out that Certifications may be issued by Certification Bodies or by the Commissioner, on the basis of criteria approved by the Commissioner.
- F. Article 42.7 sets out that Certifications can be issued for up to 3 years, and may be renewed, provided the controller or processor continues to meet the relevant requirements. It also sets out that Certifications can be withdrawn by the Certification Bodies (or by the Commissioner if the Commissioner had itself granted the Certification) where the relevant requirements are no longer met.
- G. Article 43.1 of the UK GDPR sets out that Certification Bodies must have appropriate expertise in data protection and requires that those Certification Bodies are accredited by one or both of the following:
- a) the Commissioner; or
 - b) the national accreditation body named in accordance with the Accreditation Regulations 2009 (SI No 3155/2009) and The Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019 UK Statutory Instruments 2019 No. 696 (as amended) in accordance with EN-ISO/IEC 17065/2012 (in the UK, UKAS). For the purpose of setting out the background to this Agreement we will refer to the national accreditation body in the UK as UKAS.
- H. Article 43.2 of the UK GDPR sets out specific requirements which Certification Bodies must meet (set out in Annex 1), in addition to requirements approved by the Commissioner (Art 43.3). Where Certification Bodies are accredited by UKAS, those requirements must complement those envisaged in EN-ISO/IEC 17065/2012. These requirements are to be agreed in accordance with Annex 1. The agreed requirements for the accreditation of Certification Bodies will be published by the Commissioner in accordance with Art 43.6 UK GDPR.
- I. Article 43.4 of the UK GDPR sets out that Certification Bodies may be accredited for up to 5 years, and may be renewed provided the Certification Body continues to meet the relevant requirements.
- J. Articles 43.4 and 43.5 of the UK GDPR set out that Certification Bodies are responsible for the proper assessment of controllers and processors leading to the granting, refusal, renewal or withdrawal of a Certification, and must provide reasons for granting or withdrawing a Certification to the Commissioner.

- K. Art 43.7 of the UK GDPR sets out that UKAS (or the Commissioner if the Commissioner granted the accreditation) may revoke the accreditation of a Certification Body, where the accreditation criteria are not, or no longer met, or where actions taken by the Certification Body infringe the UK GDPR.

Certification procedures under the DPA18

- L. In accordance with Section 17 DPA18:
- c) the Commissioner may only accredit Certification Bodies itself where it publishes a statement to that effect. For the time being the Commissioner does not intend to publish such a statement.
 - d) UKAS may only accredit Certification Bodies if the Commissioner publishes a statement to that effect. The Commissioner published this statement in accordance with S17(3) DPA18.
- M. Schedule 5 DPA18 sets out the procedure for reviews and appeals of decisions relating to applications or reviews of the accreditation of Certification Bodies, by those bodies.

Scope of this Agreement

- N. This Agreement sets out the terms and conditions under which the Commissioner has agreed to publish the statement that UKAS may accredit Certification Bodies, and under which UKAS has agreed to accept such a role.

Terms and conditions:

1 Interpretation

1.1 In this Agreement:

"Accreditation Services"	means the accreditation services to be performed by UKAS in accordance with the Agreement, based on the description set out in Annex 1 Part 2, and notified by the Commissioner in writing to UKAS. The Accreditation Services may be updated from time to time by the agreement of the parties in writing;
"Accreditation Requirements"	means the accreditation requirements by which Certification Bodies will be assessed and accredited, based on the principles set out in Annex 1 Part 1, as agreed in writing by the Parties. The Accreditation Requirements may be updated from time to time by the agreement of the parties in writing
"Agreement"	means this agreement between the Commissioner and UKAS and includes the Annexes;

"Certification Bodies"	means a body which performs (or which is applying to perform) assessments of controllers and processors against a set of Certification Criteria approved by the Commissioner;
"Confidential Information"	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which: (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
"Data Protection Legislation"	means all applicable data protection and privacy legislation, regulations and guidance including but not limited to the "United Kingdom General Data Protection Regulation" or "UK GDPR", the Data Protection Act 2018 ("DPA18"), the Privacy and Electronic Communications (EC Directive) Regulations and any guidance or codes of practice issued by the Information Commissioner from time to time (all as amended, updated or re-enacted from time to time);
"EIRs"	means the Environmental Information Regulations 2004;
"Environmental Information"	has the meaning given under Regulation 1(2) of the EIRs;
"FOIA"	means the Freedom of Information Act 2000;
"UK GDPR Accreditation & Certification Framework"	means the legal framework set out in the UK GDPR and DPA18 (as set out in the Background) for the Commissioner to approve UK GDPR certification schemes and UKAS to accredit certification bodies, which will grant certifications against the UK GDPR certification schemes;
"UK GDPR Certification Criteria"	means the set of requirements (or the set of requirements proposed by a Scheme Owner) against which conformity with UK GDPR is to be assessed by a Certification Body, approved (or to be approved) by the Commissioner, in accordance with the UK GDPR Certification Criteria Approval Process;
"UK GDPR Certification Criteria Approval Process"	means the process for approval by the Commissioner of proposed UK GDPR Certification Criteria, and including the UK GDPR Certification Evaluation Services, as set out in Annex 2. The UK GDPR Certification Approval Process may be updated from time to time by the Commissioner by notifying UKAS in writing;
"UK GDPR Certification Evaluation Services"	means the UK GDPR certification evaluation services to be performed by UKAS in accordance with this Agreement, as set out in Annex 2 Part 1 Para 2, as part of the UK GDPR Certification Criteria Approval Process. The UK GDPR Certification Evaluation Services may be updated from time to time by the agreement of the Parties in writing;
"Information"	has the meaning given under section 84 of the FOIA;
"Law"	means any applicable law, subordinate legislation within

	the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of sections 2-4 of the European Union Withdrawal Act 2018, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements, in each case with which a Party is bound to comply, as amended or replaced from time to time;
"Individual Contractors"	means assessors contracted by UKAS who are not its employees;
"Party"	means UKAS or the Commissioner (as appropriate) and "Parties" shall mean both of them;
"Request for Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "request" shall apply);
"Scheme Owner"	means the organisation responsible for drafting the UK GDPR Certification Criteria;
"Staff"	means all directors, officers, employees, agents, consultants and contractors of a party and/or of any sub-contractor of that party engaged in the performance of that party's obligations under the Agreement;
"Start Date"	means 1 February 2020
"Term"	means the period from the Start Date of the Agreement until it is terminated in accordance with Clause 12;
"TUPE"	means the Transfer of Undertakings (Protection of Employment) Regulations 2006;
"Working Day"	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

1.2 In this Agreement, unless the context otherwise requires:

- 1.2.1 references to numbered clauses are references to the relevant clause in this Agreement;
- 1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
- 1.2.3 the headings to the clauses of this Agreement are for information only and do not affect the interpretation of the Agreement;
- 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
- 1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Term

- 2.1 The Agreement shall take effect on the Start Date and continue unless and until it is terminated in accordance with the terms and conditions of the Agreement.

3 Collaboration by the parties

- 3.1 The parties shall collaborate to deliver the UK GDPR Accreditation & Certification Framework, and at all times act reasonably and in good faith, and shall co-operate to ensure both parties meet their legal obligations in relation to the UK GDPR Accreditation & Certification Framework.
- 3.2 The Commissioner shall consult with UKAS, and UKAS shall provide the UK GDPR Certification Evaluation Services as part of the UK GDPR Certification Criteria Approval Process in accordance with Annex 2.
- 3.3 UKAS shall provide the Accreditation Services in accordance with Annex 1, from the date the Parties agree (acting reasonably).
- 3.4 In performing its obligations under this Agreement, each party shall:
- 3.4.1 act with all reasonable care, skill and diligence in accordance with good industry practice in that party's industry, profession or trade;
 - 3.4.2 use Staff who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number, and who have been vetted in accordance with that Party's policies and procedures;
 - 3.4.3 provide its own equipment;
 - 3.4.4 ensure that it obtains, and maintains all consents, licences and permissions (statutory, regulatory, contractual or otherwise) it may require and which are necessary to enable it to comply with its obligations in the Agreement; and
 - 3.4.5 comply with all Laws.

4 Charges

- 4.1 Each party shall bear its own costs in performing its obligations under this Agreement.
- 4.2 Either party may impose charges on third parties where permitted by Law.
- 4.3 The Parties confirm that UKAS intends to charge Certification Bodies for the Accreditation Services it provides to them, in accordance with UKAS's terms and conditions and Section 17(6) of the DPA18.

5 Assignment and Sub-contracting

- 5.1 Neither Party shall, without the written consent of the other Party, assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the

Agreement or any part of the Agreement.

5.2 In exceptional circumstances, UKAS will subcontract the assessment of conformity assessment bodies. UKAS cannot subcontract the decision and awarding of accreditation. The Commissioner consents to UKAS sub-contracting the assessments to other accreditation bodies provided that:

5.2.1 such sub-contracting is in accordance with UKAS's policies and procedures, including appropriate due diligence and information security checks and regular monitoring of the sub-contractor's compliance, which may include audits;

5.2.2 For individual contractors: at any time on reasonable request, UKAS will provide the Commissioner with a copy of such contracts and the documentary evidence that UKAS has complied with its contracting policies and procedures.

5.2.3 For other sub-contractors: at the time such sub-contract is entered into, and at any time on request, UKAS will provide the Commissioner with a copy of such sub-contracts and the documentary evidence that UKAS has complied with its sub-contracting policies and procedures;

5.2.4 (subject always to its compliance with its obligations of confidentiality in accordance with Clause 8) the Commissioner is entitled to require UKAS to undertake an audit of the sub-contractors and review documentation of those audits. The Commissioner reserves the right to audit the compliance of those sub-contractors with their sub-contracts directly; and

5.4.5 UKAS remains responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.

6 Intellectual Property Rights

6.1 Each party shall retain all intellectual property rights in any materials provided by it or created by it pursuant to this Agreement.

6.2 Each Party grants the other a non-exclusive royalty free licence (including the right to sub-licence) for the term of this Agreement, to use any of its intellectual property rights, as reasonably necessary for it to perform its obligations under this Agreement and/or for the purposes of the UK GDPR Accreditation & Certification Framework.

6.3 Neither Party shall have any right to use any of the other Party's names, logos nor trade marks on any of its products or services unless such other Party's prior written consent is obtained, or such consent is expressly set out in this Agreement.

7 Governance, Audit and Records

7.1 UKAS and the Commissioner shall attend quarterly progress meetings and both shall ensure that its representatives are suitably qualified to attend such

meetings.

- 7.2 UKAS shall provide the Commissioner with a quarterly report and other information, as set out in Annex 3 at least one week before the quarterly meeting.
- 7.3 UKAS shall provide all necessary information and assistance to the Commissioner in order for the Commissioner to verify UKAS's compliance with its obligations under this Agreement including:
- 7.3.1 allowing the Commissioner and its advisors to inspect and make copies of the records required to verify compliance under this Clause 7; and
 - 7.3.2 allowing access to UKAS premises on reasonable notice and provide all reasonable assistance to the Commissioner to enable the Commissioner to audit the UKAS's compliance with this Agreement.
- 7.4 UKAS shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Accreditation Services. UKAS shall on request afford the Commissioner or the Commissioner's representatives such access to those records as may be reasonably requested by the Commissioner in connection with the Agreement.

8 Confidentiality, Transparency and Publicity

- 8.1 Subject to clause 8.2, each Party shall:
- 8.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and
 - 8.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.
- 8.2 Notwithstanding clause 8.1, a Party may disclose Confidential Information which it receives from the other Party:
- 8.2.1 where disclosure is required by applicable Law or by a court of competent jurisdiction;
 - 8.2.2 to its auditors or for the purposes of regulatory requirements;
 - 8.2.3 on a confidential basis, to its professional advisers;
 - 8.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;
 - 8.2.5 to its Staff on a reasonable need to know basis and in accordance with its usual policies and procedures for confidential information; and
 - 8.2.6 where the receiving Party is the Commissioner:

(a) to the extent that the Commissioner (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or

(b) in accordance with clause 9,

8.3 The Parties acknowledge that, except for any Information or Environmental Information which is exempt from disclosure in accordance with the provisions of the FOIA or EIRs, the content of the Agreement is not Confidential Information and UKAS hereby gives its consent for the Commissioner to publish this Agreement in its entirety to the general public (but with any Information or Environmental Information that is exempt from disclosure in accordance with the FOIA or EIRs redacted) including any changes to the Agreement agreed from time to time. The Commissioner may consult with UKAS to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA or EIRs.

8.4 UKAS shall take reasonable steps to ensure that its Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Commissioner.

9 Freedom of Information and Environmental Information

9.1 UKAS acknowledges that the Commissioner is subject to the requirements of the FOIA and the EIRs and shall:

9.1.1 provide all necessary assistance and cooperation as reasonably requested by the Commissioner to enable the Commissioner to comply with its obligations under the FOIA and the EIRs;

9.1.2 respond to the requestor in relation to their Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 3 Working Days of receipt and, where relevant, will direct the requestor to make the Request for Information to the Commissioner.

9.1.3 provide the Commissioner with a copy of all Information or Environmental Information belonging to the Commissioner requested in the Request for Information which is in its possession or control in the form that the Commissioner requires within 5 Working Days (or such other period as the Commissioner may reasonably specify) of the Commissioner's request for such Information or Environmental Information; and

9.2 The Commissioner will treat any FOI request on a case-by-case basis and will not disclose any information without requesting prior consultation with the concerned parties. The Commissioner will take due regard of any representations made by UKAS or other concerned parties. The Commissioner will consider what exemption, if any, applies including Section 41 (information provided in confidence), Section 36 (conduct of public affairs) and Section 43 (commercial interests) of FOIA.

9.3 Notwithstanding any other provision in the Agreement, the Commissioner shall be responsible for determining in its absolute discretion whether any Information relating to UKAS or the Services is exempt from disclosure in accordance with the

FOIA and/or the EIRs.

10 Data Protection

- 10.1 The Parties shall comply with their respective obligations under the Data Protection Legislation.
- 10.2 Given the nature of the Services, the Parties expect to only exchange minimal personal data, which would not warrant the inclusion of data sharing provisions in this Agreement. If this changes, the Parties shall (acting reasonably) agree a Variation Notice to govern the sharing of such personal data between them.
- 10.3 UKAS may share personal data with the Commissioner in relation to any audits conducted by the Commissioner and upon termination, when UKAS is required to transfer to the Commissioner (or a replacement provider of the Accreditation Services) such personal data as required for the continuation of the Accreditation Services. In all cases, UKAS shall ensure that such transfer is made in accordance with the Data Protection Legislation.

11 Force Majeure

- 11.1 Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Party affected. Each Party shall promptly notify the other Party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If such circumstances continue for a continuous period of more than two months, either Party may terminate the Agreement by written notice to the other Party.

12 Termination

- 12.1 Either party may terminate this Agreement on 12 month's written notice in writing.
- 12.2 Without prejudice to any other right or remedy it might have, either Party may terminate the Agreement in whole or in part by written notice to the other with immediate effect if the other Party:
- 12.2.1 is in material breach of any obligation under the Agreement which is not capable of remedy;
 - 12.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;
 - 12.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of receiving notice specifying the breach and requiring it to be remedied;
 - 12.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;

- 12.2.5 in the case of the Commissioner, ceases to have its obligations to provide the UK GDPR Accreditation & Certification Framework, and in the case of UKAS it ceases to have its status as the UK national accreditation body.
- 12.2.6 UKAS becomes insolvent, or if an order is made or a resolution is passed for its winding up (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of its assets or business, or if it makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 12.2.5) in consequence of debt in any jurisdiction.
- 12.3 Each party shall notify the other as soon as practicable if they become aware that any of the events in Clauses 12.2.4, 12.2.5, or 12.2.6 occur or are likely to occur.
- 12.4 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and any provision of the Agreement that expressly or by implication is intended to come into or continue in force on or after termination or expiry of the Agreement shall remain in full force and effect.
- 12.5 Upon termination or expiry of the Agreement, each Party shall:
- 12.5.1 give all reasonable assistance to the other for the orderly transfer of the Accreditation Services to the Commissioner (or a third party), including UKAS providing all documentation and materials relating to the accreditation of Certification Bodies which are ongoing, and any other documentation or assistance which the Commissioner reasonably requests; and
 - 12.5.2 securely return to the other Party all its Confidential Information and any other documents, information and data the other Party reasonably requests, as soon as reasonably practicable.

13 Compliance

- 13.1 Each party shall have in place, and comply with, policies and procedures which are appropriate for its status as, in the case of the Commissioner, the UK's independent regulator of data protection law, and in the case of UKAS the UK national accreditation body. Each Party shall take appropriate steps to secure the observance of its Staff with those policies and procedures.
- 13.2 UKAS shall comply with, and shall ensure that its Staff shall comply with, the provisions of:
- 13.2.1 the Modern Slavery Act 2015;
 - 13.2.2 prevention of fraud and corruption; and
 - 13.2.3 equality Law.
- 13.3 Neither party shall offer, give, agree to give, accept or agree to accept anything,

to or from any person, an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or refusal of approval of any UK GDPR Certification Criteria or accreditation of Certification Bodies, or for showing or refraining from showing favour or disfavour to any person in relation to the UK GDPR Accreditation & Certification Framework.

13.4 If UKAS or its Staff engages in conduct prohibited by clause 13.3 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Commissioner) the Commissioner may:

13.4.1 terminate the Agreement and recover from UKAS the amount of any loss suffered by the Commissioner resulting from the termination, including the cost reasonably incurred by the Commissioner of making other arrangements for the supply of the Services and any additional expenditure incurred by the Commissioner throughout the remainder of the Agreement; or

13.4.2 recover in full from UKAS any other loss sustained by the Commissioner as a direct result of any breach of this clause.

14 Dispute Resolution

14.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.

14.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 14.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the "Mediator") chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.

14.3 If the Parties fail to appoint a Mediator within one month, or fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, either Party may exercise any remedy it has under applicable Law.

15 TUPE

15.1 The Parties do not anticipate that TUPE will apply on the Start Date as a result of entering into this Agreement, so as to transfer the contracts of employment of any employees from the Commissioner to UKAS (or any of its sub-contractors).

15.2 UKAS agrees that it shall not, and procures that any of its sub-contractors shall not structure its Staff in such a way that they will be subject to a relevant transfer for the purposes of TUPE.

15.3 The Parties acknowledge and agree that TUPE is not intended to apply to any person as a consequence of the termination or expiry, in whole or in part, of this Agreement.

16 General

- 16.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.
- 16.2 A person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce or enjoy the benefit of this Agreement, except to the extent that TUPE is applicable in which case the terms of this Agreement which contain an indemnity from UKAS to the new provider of the services equivalent to the Services (or any of them) may be enforced by such new provider of the services equivalent to the Services (or any of them) after the expiry or termination of this Agreement or any Service.
- 16.3 The Agreement cannot be varied except in writing signed by a duly authorised representative of each of the Parties.
- 16.4 The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.
- 16.5 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.
- 16.6 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.
- 16.7 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement or in Law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
- 16.8 If any provision of the Agreement is prohibited by Law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.

17 Notices

- 17.1 Any notice to be given under the Agreement shall be in writing and may be served by personal delivery, first class recorded or, subject to clause 17.3, e-mail to the

following addresses:

Commissioner

Attention:
[redacted] Head of Assurance
(Supervision)
Wycliffe House, Water Lane,
Wilmslow, SK9 5AF

CC: [redacted]

UKAS

Attention:
[redacted] Chief Executive
2 Pine Trees, Chertsey Lane,
Staines-upon-Thames, TW18 3HR

CC: [redacted]

or such other address as that Party may from time to time notify to the other Party in accordance with this clause.

17.2 Notices served as above shall be deemed served on the Working Day of delivery provided delivery is before 5.00pm on a Working Day. Otherwise delivery shall be deemed to occur on the next Working Day. An email shall be deemed delivered when sent unless an error message is received or, where an out of office message is received, on the date the out of office message states the recipient is to return.

17.3 Notices under clauses 11 (Force Majeure) and 12 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 17.1.

18 Governing Law and Jurisdiction

18.1 The validity, construction and performance of the Agreement, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

Signatories

Information Commissioner's Office	UKAS
[redacted] - Director of Regulatory Assurance [redacted]	[redacted] Chief Executive [redacted]
Address: Wycliffe House, Water Lane, Wilmslow, SK9 5AF	Address: 2 Pine Trees, Chertsey Lane, Staines-upon-Thames, TW18 3HR
Signed: [redacted]	Signed: [redacted]
Date: 14.11.2022	Date: 19.10.22

Annex 1

Accreditation Requirements and Accreditation Services

Part 1: Accreditation Requirements

The Accreditation Requirements for Certification Bodies is based on the principles set out below, and is as agreed by the Parties in writing (acting reasonably).

This may be further updated by the Parties from time to time, by agreement in writing.

For the purposes of this Annex "ICO" means the Information Commissioner.

1. Underlying Principles:

Certification Bodies will be assessed against ISO/IEC 17065 together with additional requirements, referred to in Article 43(1)(b), which will

- a) demonstrate their independence and expertise in relation to the subject-matter of the certification;
- b) undertake to respect the criteria referred to in Article 42(5) and approved by the ICO;
- c) establish procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- d) establish procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- e) demonstrate, to the satisfaction of the ICO authority that their tasks and duties do not result in a conflict of interest.

2. UK Additional Accreditation Requirements for Certification Bodies

The requirements referred to in Article 43(1)(b) and point 1 above, are set out in the 'UK additional accreditation requirements for certification bodies' document published on the Commissioner's website.

Part 2: Accreditation Services

The Accreditation Services are as agreed by the parties in writing and are based on the processes set out below. This may be further updated by the Parties from time to time, by agreement in writing.

UKAS will perform the Accreditation Services in accordance with its policies and procedures, as updated by UKAS from time to time.

1. Process for the accreditation of Certification Bodies

- UKAS will receive and process applications for accreditation by Certification Bodies that wish to deliver ICO-approved UK GDPR Certification Criteria, in line

with the General Principles for the Assessment of Conformity Assessment Bodies by the United Kingdom Accreditation Service (GEN 1).

- On receipt of an application to become an accredited Certification Body, UKAS will notify the ICO and provide the organisation's details in line with the UKAS Confidentiality Waiver (Annex 4).
- As part of the accreditation process UKAS will be required to check that a Certification Body can demonstrate and provide evidence that its procedures and measures specifically for processing applicant and client organisation's personal data as part of the certification process are compliant with the UK GDPR and the UK Data Protection Act 2018 (DPA18).
- the Certification Body shall also be required to demonstrate to the accreditation body that they are not the subject of any ICO investigation or regulatory action which might prevent their accreditation. UKAS will be required to verify this with the ICO before proceeding with the accreditation process.
- UKAS will take any non-compliance with UK GDPR/DPA18 into account when deciding whether to accredit a Certification Body.
- UKAS are able to accredit Certification Bodies where they fulfil the Accreditation Requirements.
- UKAS shall ensure that any agreement between UKAS and a Certification Body accredited or seeking accreditation to the Accreditation Requirements, includes provision for UKAS to provide the Commissioner with:
 - a) details of any application(s) for such accreditation;
 - b) details of progress towards gaining accreditation(s);
 - c) information relating to the accreditation in order to allow the Commissioner to carry out their regulatory functions; and
 - d) details of any change or extension to scope(s) of accreditation.

2. Process for the hearing of appeals

Appeals will be conducted in accordance with Schedule 5 of the DPA18, and UKAS's policies and procedures for handling appeals.

3. Process for the review of the accreditation of Certification Bodies

UKAS shall undertake an annual (as a minimum) review of a certification body's accreditation. This will include an onsite component (and findings will be documented. The review will be conducted by UKAS in accordance with its policies and procedures.

Should the ICO become aware of any data protection compliance issues on the part of a Certification Body, UKAS will be notified of the nature of the concern and the supporting evidence to enable them to review the accreditation of the Certification Body.

The ICO will (acting reasonably) stipulate with the time period within which UKAS must conduct its review. This time will depend on the seriousness of the compliance issue.

Within the stipulated time period, UKAS will investigate the matter to determine if the Certification Body still meets requirements for accreditation and whether any remedial action is required.

On conclusion of the investigation UKAS will report the outcome to the ICO within 5 working days.

4. Process where UKAS suspends or revokes the accreditation of a Certification Body

UKAS will revoke accreditation where the Accreditation Requirements are no longer met, acting in accordance with its policies and procedures.

Any suspension (full or part and including voluntary suspension) or revocation of accreditation must be notified to the ICO with immediate effect.

Annex 2

For the purposes of this Annex "ICO" means the Information Commissioner.

UK GDPR Certification Criteria Approval Process

The UK GDPR Certification Criteria Approval Process, including the scope of the UK GDPR Certification Evaluation Services to be provided by UKAS as part of that process, is based on the principles set out below, and is as agreed in writing by the Parties (acting reasonably).

This may be further updated by the Parties from time to time, by agreement in writing.

Process for the approval of UK GDPR Certification Criteria

Scheme criteria will be submitted to the Commissioner by the "Scheme Owner" (the organisation which drafted the criteria).

Part 1: Initial Assessment:

There are two parts to this:

(i) The Commissioner initial assessment:

The Commissioner will perform an initial assessment of the UK GDPR Certification Criteria to determine if it satisfies key elements below:

- is laid out in a logical and understandable way;
- identifies a clear market need for the scheme;
- scope is clearly defined, meaningful and not misleading;
- scope includes all relevant aspects of processing to be addressed by the scheme criteria;
- territorial scope is defined;
- the criteria sufficiently describe how the target of evaluation (ToE) should be defined by the controller/processor;
- the criteria guarantee that the ToE will be understandable to intended audience including data subjects, for example by providing a use case;
- relevant terms defined and normative references identified;
- criteria include definition of UK GDPR responsibilities, procedures and processing covered by the scope;
- appears on first inspection to cover all relevant sections of UK GDPR that relate to the scope, ie. principles, rights, lawful basis, data protection by design and default, requirement to assess risks to rights and freedoms of individuals; and
- allows meaningful UK GDPR certification, taking into account nature, content, risk and scope of processing.

(ii) UKAS UK GDPR input to the Commissioners triage process:

Where necessary, the Commissioner will request input from UKAS into the triage process. Where this is the case, the Commissioner will forward the UK GDPR Certification Criteria and any supporting documentation to UKAS for UKAS to advise the Commissioner on specific aspects of the scheme in relation to ISO 17065

The UKAS evaluation of a complete conformity assessment scheme (as defined by the European Accreditation Cooperation (EA) document EA 1/22 "EA 1/22") will follow¹ the process and criteria set out EA 1/22. This will take place separately during the provision of the Accreditation Services by UKAS of Certification Bodies.

Both parties will agree a timeframe for the UKAS UK GDPR input to the Commissioners triage process and the response provided to the ICO, which would normally be within 5 days.

The ICO will make the decision whether or not the UK GDPR Certification Criteria is successful at this initial assessment stage, and will notify the Scheme Owner of the outcome and outline the next steps.

Part 2: ICO full assessment process

The ICO will then carry out a full assessment of the UK GDPR Certification Criteria based on the conditions laid out in Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation v3.0 issued by EDPB.

The ICO will communicate its decision to UKAS and the Scheme Owner and publish details in the Register of certification scheme criteria.

Should any changes to the criteria be necessary following an assessment by UKAS and/or pilot phase then these will be approved via the full assessment process described above.

Part 3: Reviews and amendments

The parties will collaborate and act reasonably in order to agree the process for reviews and amendments to UK GDPR Certification Criteria which have been approved, within 12 months of the Start Date (or longer if both parties agree).

¹ <https://european-accreditation.org/publications/ea-1-22-a/f>

Annex 3

UKAS Reporting

For the purposes of this Annex "ICO" means the Information Commissioner.

For ICO oversight and effective management of our agreement with UKAS the following information will be provided in writing to [REDACTED]

Quarterly (provided in standard report template):

- applications received;
- details of applicants;
- status of applications;
- accreditations refused/issued/withdrawn; and
- a summary of complaints/appeals received.

Proactively as and when and without delay/ in advance / copy ICO in on correspondence:

- On receipt of an application for accreditation by a proposed Certification Body, UKAS shall notify the ICO of the applicant details
- When issuing/renewing accreditation UKAS shall copy the ICO into the grant letter or renewal letter issued to the certification body, thereby providing the ICO with relevant details.
- Details of any suspension, or withdrawal of accreditation, whether voluntary or imposed; and
- Details of any nonconformity by a Certification Body with the Accreditation Requirements which in the opinion of UKAS has the potential to lead to suspension or withdrawal of accreditation, or could result in an infringement of the UK GDPR or damage to the integrity of UK GDPR Certification Criteria.

Annex 4

UKAS Confidentiality Waiver



**THE ACCREDITATION OF CERTIFICATION BODIES DEVELOPING DATA PROTECTION
CERTIFICATION MECHANISMS FOR THE PURPOSE OF DEMONSTRATING COMPLIANCE
WITH THE GENERAL DATA PROTECTION REGULATION (UK GDPR) -
Confidentiality Waiver**

It is acknowledged that in accordance with the terms of the agreement between the Information Commissioner's Office (ICO) and United Kingdom Accreditation Service (UKAS) it will be necessary for UKAS to reveal the following information to the ICO:-

- a) details of any application for accreditation;
- b) details of progress towards gaining accreditation; and
- c) details of progress towards extension to scope of accreditation.

In addition, UKAS will, in every instance, provide the ICO with:

- a) details of any suspension or withdrawal of accreditation, whether voluntary or imposed; and
- b) details of any non-conformity with the Standard (ISO/IEC 17065) and/or the Commissioner's certification criteria which in the opinion of UKAS has the potential to lead to suspension or withdrawal of accreditation, or could result in any breach of the UK GDPR¹

Therefore, to comply with the terms of the agreement, and in this instance only, UKAS is authorised to reveal such information as meets the terms and conditions of the agreement.

It is to be understood that UKAS will in all other respects comply with the confidentiality clauses in the agreement signed between this provider and UKAS.

Also, it is to be understood that the ICO will comply with Sections 7 and 8 of their agreement with UKAS using any information supplied by UKAS only as necessary for the discharge of their regulatory functions.

Signature _____

Name _____

Position _____

Date (select) _____

For and on behalf of:-

Organisation _____

UKAS Accreditation No. _____

¹ If in doubt UKAS should liaise with the ICO using redacted data in order to maintain confidentiality but alerting the ICO to potential quality issues so that effective decisions can be made.