Data Processing Agreement
for
CAE's Training Centre Management System (TCMS) and-or
CAE's Qualification Test Guide (QTGx)

This Data Processing Agreement ("DPA") is incorporated into and forming part of the Commercial Agreement (as defined below) between CAE and Customer (as defined in the Agreement) for the purchase of CAE Services (as defined below) and is made as of the Effective Date (as defined below).

Capitalized terms used but not defined in the DPA or the Commercial Agreement will have the meaning ascribed thereto in the Data Protection Law.

The Parties have agreed on the following DPA in order to provide Appropriate Safeguards with respect to the protection of privacy for the transfer of Personal Data by the Customer to CAE as specified in Annex I.

This DPA will be deemed legally binding upon receipt by CAE of a fully executed copy of the Commercial Agreement between Customer and CAE.

How This DPA Applies - Order of Precedence.

In the event of any conflict between the following documents, and only to the extent of such conflict, the order of precedence will be as follows:

(a) between the Commercial Agreement and the DPA, the DPA will prevail;

(b) between (i) the DPA and (ii) the EU Clauses, Swiss Clauses and/or UK Addendum, the EU Clauses, Swiss Clauses and/or UK Addendum (as applicable) will prevail.

This DPA is divided into three parts:

Part I - Definitions;

Part II - General data protection provisions;

Part III - Additional provisions for specific Data Protection Laws.

Part I - Definitions

"Affiliate" means any and all legal entities with respect to which the ultimate parent of that entity, at present or in the future, either directly or indirectly, holds more than 50 percent of the nominal value of the issued share capital, or more than 50 percent of the voting power at general meetings, or has the power to appoint and to dismiss a majority of the managing directors or otherwise to direct the activities of such entity (and provided an entity is not subject to a separate agreement with CAE).

"Anonymized Data" means data that has been appropriately and effectively anonymised in accordance with the requirements of the Data Protection Law, so that it no longer constitutes Personal Data.

“Appropriate Safeguards” means the standard of protection over the personal data and of data subjects’ rights, which is required by Data Protection Laws.

“Approved Addendum” means the template UK Addendum for the transfer of personal data to third countries (International Data Transfer Addendum to the EU Standard Contractual Clauses) issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it may be updated, amended or replaced from time to time.

"Approved EU Clauses" means the standard contractual clauses for the transfer of personal data to third countries, pursuant to European Commission Decision 2021/914/EU in the form of the Controller to Processor Module II and as they may be updated, amended or replaced from time to time.

“**CAE Services**” means the services offered by CAE to the Customer in accordance with the Commercial Agreement, including CAE’s Training Centre Management System (TCMS) and-or CAE’s Qualification Test Guide (QTGx).

“CCPA” means the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq., as updated, amended or replaced from time to time.

“**Commercial Agreement**” means collectively, the Software as a Service – QTGX and-or TCMS Commercial Agreement between CAE and the Customer dated as of the Effective Date (as such term is defined in the Commercial Agreement), which may include a software as a service solution allowing the management of a training center daily activities (TCMS), and-or a cloud-based software as a service which enables the user to manage the entire Qualificaton Test Guides lifecyle more efficiently through a digital solution (QTGx), and any future work orders or agreements entered into between the Customer and CAE in connection therewith, in each case as updated,amended, restated or replaced from time to time.

“Consumer” as defined under the CCPA.

“Controller” as defined under the GDPR or UK GDPR.

"Data Protection Law" means all applicable data protection and privacy laws protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data including but not limited to the the CCPA, the GDPR, the UK GDPR and the PIPEDA.

"Data Subject" as defined under the GDPR or UK GDPR.

"Data Subject Request" means a request from or on behalf of a Data Subject relating to access to, or rectification, erasure, restriction or data portability in respect of that person`s Personal Data or an objection from or on behalf of a Data Subject to the processing of its Personal Data.

“EU Clauses”: means the Approved EU Clauses as interpreted in Annex IV.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as updated, amended or replaced from time to time.

"ICO" means the UK Information Commissioner's Office.

"Personal Data" means all data which is defined as 'personal data' under the Data Protection Law and which is processed by CAE as a Processor as part of its provision of the CAE Services to Customer.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data while being transmitted, stored or otherwise processed by CAE.

"PIPEDA" means the Canadian Personal Information Protection and Electronic Documents Act of 2000 as updated, amended or replaced from time to time.

"Process" or "Processing" as defined under the Data Protection Law.

"Processor" as defined under GDPR or UK GDPR.

"Restricted Transfer" means a transfer which is covered by Chapter V of the GDPR or and/UK GDPR (as relevant).

"Sell" as defined under the CCPA.

"Supervisory Authority" as defined under the Data Protection Law.

"Swiss Clauses" means the EU Clauses as adapted in Annex V.

"Swiss Data Protection Law" means the Federal Act on Data Protection of 19 June 1992 (SR 235.1; FADP) and its revised version of 25 September 2020 ("Revised FADP"), which is scheduled to come into force on 1 January 2023, as updated, amended or replaced from time to time.

"UK Addendum" means the Approved Addendum as intepreted and adapted in Annex VI.

"UK GDPR" as defined in section 3 of the UK Data Protection Act 2018, as updated, amended or replaced from time to time.

"UK Data Protection Laws" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018, as updated, amended or replaced from time to time.

Part II - General data protection provisions

The below terms and conditions apply to the Processing of Personal Data by CAE.

1. **Processing of Personal Data**
   - **1.1. Roles:** Customer is the Controller and CAE is the Processor of the Personal Data Processed by CAE under or otherwise in connection to the Commercial Agreement.
   - **1.2. CAE Responsibilities:** CAE agrees that it (and its sub-processors) will: (a) Process Personal Data only on Customer's documented instructions, such as those set forth in the Commercial Agreement and this DPA or as otherwise provided by Customer from time to time, unless CAE is required to do otherwise by applicable laws to which CAE is subject; (b) ensure that only authorized persons who are under written obligations of confidentiality have access to or otherwise Process such Personal Data; and (c) take and maintain throughout the Processing of Personal Data appropriate technical and organizational measures to secure the Personal Data, in accordance with Data Protection Law, as set forth in the Annex II herein (Technical and Organizational Measures). CAE further agrees that it will comply with the Data Protection Law applicable to CAE in the provision of CAE Services under the Commercial Agreement and this DPA.
   - **1.3. Customer Responsibilities:** Customer agrees that if it submits Personal Data to CAE when using the CAE Services, it will: (a) do so in accordance with the requirements of the Data Protection Law applicable to Customer; and (b) provide only instructions to CAE for the Processing of Personal Data that comply with such Data Protection Law. Customer shall ensure that it has established a lawful basis under applicable Data Protection Law in respect of the Personal Data it shares with CAE in order for CAE to process it in accordance with the terms of this DPA. Customer agrees not to transmit or store any other categories of Personal Data than listed in Annex I when using the CAE Services.
   - **1.4. Details of Processing Activities:** The nature and extent of Processing Personal Data by CAE to deliver the CAE Services shall be determined and controlled solely by Customer. Annex I sets out the subject matter, duration, nature and purpose of the Processing of Personal Data. The categories of Data and Data Subjects whose Personal Data may be Processed by CAE are also set forth in Annex I.

2. **Sub-processing**
   - **2.1. Sub-processors:** Customer grants CAE a general authorization to engage the companies listed in Annex III as sub-processors to support the performance of the CAE Services.
   - **2.2. Right to Object to New Sub-processors:** CAE shall inform the Customer in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 business days in advance, thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). If Customer has a reasonable objection to any new sub-processor, it shall notify CAE of such objection in writing within ten (10) business days of CAE`s advance notification. Within thirty (30) days after receipt of Customer`s objection to a new sub-processor, the Parties will seek to resolve the matter in good faith. If CAE is able to provide the CAE Services to Customer under the Commercial Agreement without using the objected to sub-processor and decides in its discretion to do so, then Customer`s objection to the sub-processor will be deemed resolved.
   - **2.3. Obligations of and Liability for Sub-processors:** Prior to engaging a sub-processor, CAE will enter into a written contract with that sub-processor, which shall include data protection provisions which are the same in substance as those in this DPA and as required by Data Protection Law. CAE agrees to be fully liable for the acts or omissions of its third-party sub-

processors to the same extent as CAE would be liable if performing the services of the sub-processors itself subject to the terms of the Commercial Agreement.

2.4. International transfers: Where CAE engages a sub-processor in accordance with this Section 2 for carrying out specific processing activities to support the performance of the CAE Services and those processing activities involve a international transfer of personal data within the meaning of Data Protection Law, CAE will ensure on the basis of a written contract or any other legitimate mean the compliance with the Data Protection Law.

3. Data Subject Requests

3.1. If CAE receives a Data Subject request from Customer`s Data Subject, it will promptly notify Customer. CAE will refrain from responding to the Data Subject except to acknowledge receipt of the request, to which Customer hereby agrees. Upon request, CAE will provide reasonable assistance to help Customer respond to a Data Subject request. CAE reserves the right to charge for assistance to the extent where CAE is instructed by Customer to respond to the Data Subject directly, on a time and material basis. Requests for assistance from CAE hereunder should be made to dataprotection@cae.com.

4. Assistance

4.1. CAE will provide assistance to Customer as Customer reasonably requests (taking into account the nature of Processing and the information available to CAE) in relation to Customer`s obligations under Data Protection Law with respect to: (a) data protection impact assessments (as such term is defined in Data Protection Law); (b) Customer`s compliance with its obligations under Data Protection Law with respect to the security of Processing; and (c) any prior consultations required with a Supervisory Authority. Requests for assistance from CAE hereunder should be made to dataprotection@cae.com.

5. Deletion or Return of Personal Data

5.1. Upon termination of the CAE Services, Customer may at its sole option, instruct CAE to return to Customer and delete, any Personal Data of the Customer Processed by CAE under the Commercial Agreement with the exclusion of any Anonymized Data derived therefrom. In the event CAE is required under applicable law to retain Personal Data Processed under this DPA after termination of the Commercial Agreement, CAE will protect the Personal Data as set forth in Section 7 (Technical and Organizational Measures).

6. Inspections and Audit

6.1. CAE will contribute to audits requested by Customer, not more than once annually (except in the event of a Personal Data Breach or request from a Supervisory Authority) to demonstrate CAE's compliance with its obligations under this DPA by: (a) providing to Customer (or Customer`s independent third-party auditor that is not a competitor of CAE) a copy of the relevant and most recent third-party audit reports or certifications, or such other written documentation generally provided by CAE if the CAE Services are not audited by a third-party; and (b) such additional information in CAE's possession or control requested or required by a Supervisory Authority to demonstrate its compliance with the data Processing activities carried out by CAE under this DPA.

6.2. If Customer is required under Data Protection Law to request any further information to confirm CAE`s compliance with its obligations under this DPA, such additional information (including any on-site inspections) will be provided and/or conducted. Customer and CAE will mutually agree upon the scope, timing and duration of any on-site inspection, including

with respect to any third-party inspector selected by the Customer. Customer will promptly notify CAE of any non-conformance discovered during an on-site audit.

6.3. Each Party will bear its own costs with respect to any inspections or audits as provided herein. Requests for any inspections or audits as provided herein shall be made to dataprotection@cae.com.

7. Technical and Organizational Measures

CAE provides the technical and organizational measures required under Data Protection Law for the security of the Personal Data it Processes as set forth in the Annex II herein.

8. Personal Data Breach

8.1. Personal Data Breach Notification: CAE will notify Customer without undue delay after becoming aware of a Personal Data Breach. Where appropriate in respect of any Personal Data which has been the subject of a Personal Data Breach, CAE will provide reasonable assistance to Customer to the extent required for Customer to comply with Data Protection Law, and providing a description of the Personal Data Breach, including where possible: (a) the nature of the Personal Data Breach and the categories and approximate number of Data Subjects and/or Personal Data records concerned; (b) the name and contact details of CAE data protection officer or other contact point; (c) a description of the likely consequences of the Personal Data Breach; and (d) to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects and provide to Customer a description thereof. Where, and in so far as, it is not possible to provide the above information at the same time, further information will be provided without undue further delay as it becomes available.

8.2. Customer Notification to CAE: If Customer determines that a Personal Data Breach must be notified to any Supervisory Authority, Data Subject, or the public under Data Protection Law, to the extent such notice makes reference to CAE, Customer agrees to consult with CAE in good faith and in advance and consider any clarifications or corrections CAE may reasonably request to the notification consistent with Data Protection Law.

9. Anonymized Data.

CAE shall strictly comply with Data Protection Law and the confidentiality provisions of the Commercial Agreement with respect to Anonymized Data. CAE may use Anonymized Data for maintenance of the Systems, performance monitoring, analytics, benchmarking, as well as improvement or optimization of the Systems or Services including through the use of artificial intelligence tools.

10. General

10.1. CAE will inform Customer, immediately upon becoming aware, if in CAE's opinion any instructions provided by Customer under this DPA infringe Data Protection Law.

10.2. CAE's aggregate liability to Customer arising out of or related to the DPA will be subject to the same limitations and exclusion of liability as apply under the Commercial Agreement, whether liability arises under the Commercial Agreement or this DPA.

10.3. This DPA will be governed by and construed in accordance with the governing law provisions set forth in the Commercial Agreement.

10.4. This DPA shall remain in full force and effect until the earlier of (i) the expiration or earlier termination of the Commercial Agreement and (ii) the mutual agreement of the Parties to terminate.

10.5. This DPA may be executed electronically and in counterparts, which counterparts taken together shall form one legal instrument.

Part III - Additional Provisions for specific Data Protection Laws

To the extent that Personal Data were subject to the GDPR ("EU Personal Data"), the Swiss Data Protection Law ("Swiss Personal Data") and/or the UK GDPR ("UK Personal Data") prior to its Processing by CAE:

1. If applicable, transfers of such Personal Data from Customer to CAE shall be based on an adequacy decision that is rendered by, respectively, the European Commission, the Swiss Federal Data Protection Authority and/or an adequacy regulation issued by the UK Government (as applicable).
2. To the extent transfers of such Personal Data from Customer to CAE are not covered by adequacy under section 1 above, the Parties hereby enter into:
   (i) for EU Personal Data, the EU Clauses;
   (ii) for Swiss Personal Data , the Swiss Clauses and/or;
   (iii)for UK Personal Data, the UK Addendum,
   with Customer acting as a data exporter and CAE as a data importer and the information required under these clauses set out in Annexes IV, V and VI.
3. CAE will promptly notify Customer if it determines that it can no longer meet its obligations under the EU Clauses, Swiss Clauses or the UK Addendum.
4. If another legal mechanism for transfers of Personal Data from Customer to CAE becomes available under the above listed Data Protection Laws, the Parties will cooperate in good faith to review and if appropriate to adopt such data transfer mechanism.

To the extent that Personal Data were subject to the CCPA prior to its Processing by CAE:

1. Roles and Responsibilities
   1.1. CAE is a "service provider" for the purposes of the CAE Services it provides to Customer pursuant to the Commercial Agreement, according to the meaning given to that term in Section 1798.140 of the California Civil Code, as of the date of execution of this DPA.
   1.2. CAE agrees that, to the extent that Customer discloses a Consumer`s Personal Information to CAE, CAE will Process that Personal Information only on behalf of Customer and pursuant to the Commercial Agreement and this DPA.
2. CAE Processing of Personal Information of Consumers
   2.1. CAE certifies that it shall not Process, retain, use, or disclose a Consumer`s Personal Information for any purpose other than for the specific purpose of performing the CAE Services specified in the Commercial Agreement.
   2.2. CAE agrees that is shall not Sell a Consumer`s Personal Information.
   2.3. CAE certifies that it understands the restrictions set forth in Section 1798.140(w)(2)(A) of the California Civil Code, as of the date of execution of this DPA, and will comply with them.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Name and contact information:** Customer as stipulated in the section “The Parties” of the Agreement.

Activities relevant to the data transferred under these Clauses: Information transfer as required to receive the CAE Services from the data importer as per the Commercial Agreement.

Signature and date: Signatures are provided in the Section ”Signatures” of the Agreement.

Role (controller/processor): Controller

Data importer(s):

1. **Name and contact information:** CAE as stipulated in the section “The Parties” of the Agreement.

Activities relevant to the data transferred under these Clauses: Processing operations as required to deliver the CAE Services to the data exporter as per the Commercial Agreement.

Signature and date: Signatures are provided in the Section “Signatures” of the Agreement.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of Data Subjects whose personal data may be transferred shall include the following, (as applicable pursuant to the specific CAE Services being offered by CAE to the Customer):

- Personnel of Customer and other individuals who use and access the systems and whose activities are managed using the systems.

Categories of personal data transferred

Categories of Personal Data transferred shall include the following, (as applicable pursuant to the specific CAE Services being offered by CAE to the Customer):

- Customer end user accounts – name and optional business contact information (phone number, mobile phone number, or corporate email address) of Customer personnel.

- Customer personnel information – information relating to the activities of Customer personnel in relation to the performance of their duties and optional business contact information (phone number, mobile phone number, address or email address).

Categories of sensitive personal data transferred

Categories of Sensitive Personal Data transferred shall include the following, (as applicable pursuant to the specific system settings that the Customer has chosen for and the CAE Services being offered by CAE to the Customer):

- Customer end user accounts and Customer personnel information – absence status including reason for absence such as sick leave of Customer personnel.

Other than mentioned above the data exporter shall not transfer to the data importer certain special categories of Personal Data in connection with the provision of the CAE Services under the Commercial Agreement.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous.

Nature of the processing

For the purpose of managing data exporter's business using the products and services provided by the data importer, and including without limitation activity such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing

The provision of hosted technology solutions to Customer for the purposes of managing its Training Center business, including but not limited to managing the activities of its personnel, the whole as set out in the Commercial Agreement and any related product specifications.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

CAE will retain and process the Personal Data for the term of the Commercial Agreement and in accordance with the provisions of this DPA regarding the return or deletion of the Personal Data.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Please refer to sub-processors as set forth in Annex III. Data exporter determines the subject-matter, nature and duration of the Processing and data importer's sub-processors Process Personal Data as required to deliver the CAE Services. CAE will retain and Process the Personal Data for the term of the Commercial Agreement and in accordance with the provisions of this DPA regarding the return or deletion of the Personal Data.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of EU Clauses:

Supervisory Authority of Ireland

ANNEX II

Technical and organizational measures

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

Data importer provides the technical and organizational measures required under Data Protection Law, as defined in the DPA, for the security of the Personal Data it processes as set forth in the Commercial Agreement. The specific technical and organizational measures are listed below:

1. Defining, publishing and communicating to staff and sub-processors a set of policies for information security.

2. Reviewing policies for information security planned intervals or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

3. Performing pre-hire screening and background checks consistent with local hiring practices and laws.

4. Holding staff with access to Personal Data accountable for maintaining confidentiality obligations.

5. Requiring business ethics, data security, and international data privacy training upon initial hire and at least annually.

6. Making copies of security standards and procedures available to all staff.

7. Establishing an appropriate access control policy and reviewing it based on business requirements and related information security requirements.

8. Assigning responsibility for information security practices and standards as part of an information security program.

9. Granting the minimum necessary logical access necessary to support the data Processing services.

10. Removing access for terminated staff promptly.

11. Requiring regular password changes for staff with access to Personal Data.

12. Requiring secure log-on procedures to access to Personal Data.

13. Controlling changes to data importers information processing facilities and information systems that affect Personal Data.

14. Monitoring the capacity and availability of information resources that store, Process or transmit Personal Data.

15. Limiting physical access to data centres processing personal data to authorized individuals supporting the physical equipment or facility; including data centre physical and environmental protections including 24x7 video surveillance; require visitor pre-authorization and full- time accompaniment at all times.

16. Protecting facilities against reasonable physical and environmental threats such as natural disasters, fires, etc.

17. Destroying physical media using industry standard practices; encrypting backups if using removable tape or other media.

18. Providing network protections like firewalls, intrusion detection and monitoring for unauthorized access.

19. Securing Personal Data transmitted over the internet and between external networks with industry standard encryption.

20. Periodically conducting vulnerability tests; regularly applying security patches; implementing malware protection for servers and workstations.

21. Data importer will not materially decrease the overall security of the data Processing services during the term of the DPA.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a Processor to a sub-processor, to the data exporter

Data importer requires that any sub-processor it engages to provide the CAE Services on its behalf in connection with the DPA does so only on the basis of a written contract which imposes on such sub-processor terms no less protective of Personal Data than those imposed on data importer in the DPA, including the transfer of Personal Data to a third country or international organization in accordance with Data Protection Law.

ANNEX III

List of sub-processors

This Annex must be completed based on the authorized subcontractors as per (Clause 9(a)).

The controller has authorized the use of the following sub-processors in connection with the provision of the CAE Services:

Sub-processor List

Entity	**Type of Service**	**Location**
CAE Group Companies	CAE Services	various location
Microsoft Azure	Hosting Services	North East USA data centre

ANNEX IV

EU Clauses

To the extent the Customer transfers EU Personal Data to CAE, in a third country which does not offer an adequate level of protection under Art. 45 GDPR, the Approved EU Clauses are incorporated into this DPA by reference and will apply between the Parties as though they were set out in this DPA in full. The Approved EU Clauses shall apply as interpreted in the follwing:

(a) For the purposes of thes Approved EU Clauses: (a) Customer is the "data exporter"; and CAE is the "data importer".
(b) "Docking Clause" under Clause 7 of the Approved EU Clauses is not included.
(c) CAE obligations in respect of erasure in Clause 8.5 of the Approved EU Clauses are supplemented by Part II - Section 5 of the DPA (Deletion or Return of Personal Data).
(d) Customer's rights under Clause 8.9(c) of the Approved EU Clauses may be exercised as set out in Part II - Section 6 of the DPA (Inspections and Audit).
(e) The Parties select Option 2 under Clause 9(a) and Customer's rights under Clause 9(a) of the Approved EU Clauses may be exercised as set out in Part II - Section 2 of the DPA (Sub-processing).
(f) "Redress" under Clause 11 of the Approved EU Clauses, the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.
(g) "Governing Law" under Clause 17 of the Approved EU Clauses, the parties select the law of Ireland.
(h) "Choice of forum and jurisdiction" under Clause 18 of the Approved EU Clauses, the parties select the courts of Ireland.
(i) the information required in the Appendices of the Approved EU Clauses is as follows:
    a. Annex I, Part A, B and C shall be deemed completed with the information set forth in Annex I, Part A, B and C of this DPA correspondingly.
    b. Annex II shall be deemed completed with the information set forth in Annex II of this DPA.
    c. Annex III shall be deemed completed with the information set forth in Annex III of this DPA.

ANNEX V

Swiss Clauses

To the extent Customer transfers Swiss Personal Data to CAE, in a country outside Switzerland which is not deemed to provide an adequate level of data protection under Swiss Data Protection Law, the EU Clauses as adapted in this Annex V shall apply:

(a) the below mentioned terms of the EU Clauses shall be interpreted in accordance with the following:
   a. "GDPR" means the Swiss Data Protection Law;
   b. the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c; and
   c. "supervisory authority" means the Federal Data Protection and Information Commissioner ("FDPIC"); and

(b) the EU Clauses will also protect the data of legal persons until the entry into force of the Revised FADP.

ANNEX VI

UK Addendum

To the extent that Customer transfers UK Personal Data to CAE in a country outside the United Kingdom which does not provide an adequate level of protection by virtue of a UK adequacy regulation, each Party agrees to be bound by the terms and conditions set out in this UK Addendum, as if though these were set out in full in this DPA, in exchange for the other Party also agreeing to be bound by this UK Addendum.

(a) The UK Addendum shall be appended to the Approved EU Clauses and include the same selections and modules as set out in Annex IV above. The relevant provisions of the UK Addendum are incorporated by reference into this DPA and are an integral part of this.

(b) For the purposes of the UK Addendum, as permitted by clause 17 of such Addendum, the Parties agree to change the format to the information set out in Part 1 of such Addendum, so that:

Part 1: Tables

The Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum. They do so by agreeing to the change herein in writing, as the change does not reduce the Appropriate Safeguards.

a. The details of the parties in table 1 shall be as set out in Annex I (Part A) of this DPA (with no requirement for signature);

b. For the purposes of table 2, the UK Addendum shall be appended to the Approved EU Clauses (including the selection of modules, the selection and/or disapplication of optional clauses, and the option for clause 9 as noted under Annex IV above);

c. The appendix information listed in table 3 shall be deemed completed as follows: (i) Appendix 1 of the UK Addendum shall be deemed completed with the information set out in Annex I of this DPA (Details of Processing) and Appendix 2 of the UK Addendum shall be deemed completed with the information set out in Annex III of this DPA;

d. Ending the UK Addendum when the Approved Addendum changes

Parties that may end this UK Addendum as set out in Section 16 are the data importer and the data exporter. (Table 4)

Part 2: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template UK Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 as it may be updated, amended or replaced from time to time.