CASEWARE
Data Processing Agreement

Version: 2.0
Last Updated: October 2022

1. Introduction & Scope

This Data Processing Agreement ("**DPA**") is incorporated by reference into the Master Product and Services Agreement ("**MPSA**") entered into by Caseware International Inc, and/or Caseware Cloud Ltd. (collectively "**Caseware**" or the **"Processor")** and the customer identified therein (the "**Customer**" or "**Controller**"). This DPA sets out the terms that apply if Personal Data (defined below) belonging to Customers established in the European Economic Union (EEA), the United Kingdom (UK) or Switzerland is processed by Caseware.

As the Processor may have access to Personal Data in providing Services (defined below), the Customer (as the Controller) and Caseware (as the Processor) require a contractual agreement concerning the collection, processing and use of personal data accessed by the Processor to ensure the personal data receives protection equivalent to that afforded by the Controller. This DPA governs the duration of the processing, the nature and purpose of the processing, the type of Personal Data being processed, the categories of Data Subjects and the rights and obligations of the Controller and of the Processor.

Customer and Caseware are separately referred to as "**Party**" and collectively as "**Parties**".

2. Definitions

Capitalized terms not defined in this DPA shall have the meaning given to them in the MPSA.

- **"Data Protection Laws"** shall mean all data protection and privacy laws applicable to the processing of Personal Data according to the territorial origin of the Personal Data.

- **"Data Subject"** shall mean an identified or identifiable natural person related to the Personal Data.

- **"Personal Data" or "personal data"** shall mean, for the purposes of this DPA, any information relating to an identified or identifiable natural person.

- "**Privacy Statement**" means the privacy statement adhered to by Caseware in provision of all Caseware Offerings, as published and updated from time to time on www.caseware.com.

- **"Restricted Transfer"** shall mean (i) a transfer of Personal Data from Customer to Caseware; or (ii) an onward transfer of Personal Data from Caseware to a Sub-Processor, or iii) an onward transfer between two establishments of Caseware or a Sub-Processor; in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws), authorization mechanisms will be applied as required by applicable Data Protection Laws.

- **"Services"** shall mean services offered by Caseware with respect to software provided by Caseware as a service (as defined in the MPSA), or software licensed to the public, and shall include any software support services provided by Caseware or its Affiliates.

- **"Standard Contractual Clauses"** shall mean the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council approved by decision of the European Commission of 4.6.2021. 2.7.

- **"Sub-Processor"** shall mean any person or entity appointed by or on behalf of Caseware to process Personal Data on behalf of Caseware in connection with the Services and shall include any Sub-Processor rightfully appointed by a Sub-Processor (a Sub-Sub-Processor) to process Personal Data on behalf of Caseware in connection with the Services but shall not include any individual employee of Caseware or a Sub-Processor.

3. Details of the Processing

Caseware will collect, use, and disclose Personal Data in accordance with the Privacy Statement.

4. Type of Data

The following types/categories of data that may be collected, processed and/or used by Caseware include:

- Personal Data (e.g., last name, first name, address and date of birth);
- Communication data (e.g., telephone number, email);
- Contract data (e.g., billing and payment details);
- IT usage data (e.g., user ID, passwords and roles);
- Bank data (e.g., bank account details and credit card number); and/or
- Any other category set out in the Privacy Statement.

5. Data Subjects

Data Subjects which may be affected by using their Personal Data include:

- The Customer's clients/service recipients;
- The Customer's employees; and/or
- The Customer's suppliers/service providers.

6. Place of Data Processing

Caseware uses third party data hosting providers such as Amazon Web Services (AWS) to host the Services and to act as Sub-Processors on servers located throughout the world. At present, Caseware uses servers in Australia, Canada, Ireland and the United States.

At the time of subscribing to Caseware Services, Customer will be advised as to the geographic server that will host Personal Data and will be given an opportunity to consent thereto prior to Personal Data of Customer being stored with any such data hosting provider.

Caseware will reasonably attempt to allocate a server in a geographically proximate location to the Customer so as to avoid cross-border transfer of the Personal Data. Where that is not possible, legally required authorization mechanisms will be applied with the consent of the Customer, including for the provision of technical support and maintenance services requested by the Customer.

7. Instructions

Caseware shall process Personal Data for the purposes of: (i) processing as required by Customers in their use of the Services; (ii) processing in accordance with the MPSA, this DPA and any other agreements between the Parties, (iii) processing to comply with other reasonable instructions provided by Customer where such instructions are consistent with the terms of the MPSA, applicable laws and DPA. Caseware will inform Customer if, in Caseware's opinion, the Customer's instructions or requests are contrary to Data Protection Laws, with reasons therefore by email.

8. Confidentiality Commitment by Caseware

Caseware will ensure (a) the reliability of all individuals who could potentially access the Personal Data through background checks; (b) that all such individuals are subject to confidentiality undertakings at least as restrictive as those set forth in the MPSA and will treat the Personal Data as Confidential Information; and (c) that all such individuals have undergone training in the care, protection, and handling of Personal Data.

9. Technical & Organizational Measures

Caseware shall implement the necessary technical and organizational measures ("**TOMs**") to ensure a level of security appropriate to the risk. These may include, as appropriate:

- the pseudonymization and encryption of Personal Data;
- availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing and must maintain these measures for the duration of the contract.

Caseware will implement appropriate technical and organisational measures to protect Customer's Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. When implementing and updating such technical and organisational measures ensuring a level of security appropriate to the risk, Caseware will have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Without limiting the generality of the foregoing, Caseware has carried out the technical and organizational measures ("**TOMs**") specified in **Attachment 1** to this DPA.

Caseware engages approved Sub-Processors to provide parts of the Services. The TOMs therefore depend partially on these Sub-Processors, as also described in **Attachment 1,** provided that Caseware remains responsible for its compliance with the TOMS regardless of its reliance on Sub-Processors**.** Caseware may decide on commercially reasonable improvements of the TOMs and provide the Customer on request with an updated **Attachment 1**.

10. Global Privacy Officer

Caseware has appointed its Sr. Director of Legal as Caseware's Global Chief Privacy Officer.

11. Sub-Processors

Customer acknowledges and agrees that Caseware may engage Sub-Processors in the provision of Services, subject to the terms and conditions of this DPA, and that (i) a Caseware Affiliate may be retained as a Sub-Processor; and (ii) Caseware or a Caseware Affiliate may engage third-party Sub-Processors.

Where Caseware engages a Sub-Processor in the provision of Services, a data processing agreement will be entered into with the Sub-Processor. A list of Caseware's current Sub-Processors is available in **Attachment 2**.

Caseware will review and update the list of Caseware`s Sub-Processors on an annual basis and provide Customers with written notice of any applicable updates. Within ten (10) business days of an update to the list of Sub-Processors, Customer shall inform Caseware, in writing, of objections to any new Sub-Processors. If Customer objects to a new Sub-Processor, even though the new Sub processor is necessary for Caseware and Services, then Customer may terminate any subscription for the affected Caseware Cloud Services without penalty by providing, before the end of the notice period, written notice of termination.

If use of a Sub-Processor involves a Restricted Transfer, Caseware shall ensure that the authorization required under applicable law are at all relevant times incorporated into an agreement between Caseware and the Sub-Processor; and between the Sub-Processor and any Sub-Sub-Processor.

12. Data Subject Requests

Caseware shall reasonably support the Customer in the case of a data subject access, rectification or erasure requests, insofar as Customer cannot fulfill such a request on its own, to the extent legally permitted and technically possible. Customers shall pay Caseware costs for such support, to the extent legally permitted.

If a data subject request is received by Caseware that relates to Personal Data transferred by the Customer, Caseware will refer the request to the Customer. Caseware will not respond to such a request but shall instead support Customer as provided in this Section.

13. Data Breach Notification

Caseware shall inform Customer without undue delay, and no later than 72 hours, after becoming aware of a breach of the Personal Data (meaning a breach of security leading to destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed), including a breach at a Sub-Processor, and shall provide the necessary information to allow Customer to inform authorities and data subjects. Caseware shall take reasonable efforts to remediate the causes of such data breach and mitigate (potential) damage resulting from the breach.

The notification to Customer will include at least a) the nature of the breach, b) the impacted data categories, c) the identified and potential consequences of the breach and d) the measures Caseware takes to mitigate the consequences of the breach. At the request of Customer, Caseware shall assist Customer in notifying the breach to a supervisory authority and/or the data subjects concerned.

14. Data Protection Impact Assessment (DPIA)

Upon request by Customer, Caseware shall provide reasonable assistance to Customer in conducting a DPIA, solely in relation to Caseware's processing of Customer's Personal Data and taking into account the nature of the processing and information available to Caseware and Sub-Processors. Customers shall pay Caseware costs for such support, to the extent legally permitted.

15. Deletion or Returning Personal Data

Caseware shall, at the choice of Customer, irretrievably delete or return all Personal Data within 120 calendar days of termination or expiry of the MPSA with Customer, unless storage of the data is required by law.

16. Information & Audit Rights

Customers may obtain information on existing Caseware security certifications at *https://www.Caseware.com/cloud-security-compliance*. Upon Customer's request, Caseware shall make available to Customer, or a third-party auditor instructed by Customer, once a year, information regarding Caseware's compliance with this DPA and Data Processing Law, including onsite audits. Any audit may include Caseware submitting its data processing facilities, data files and documentation needed for processing Personal Data (and/or those of its agents, affiliates and Sub-Processors) to reviewing, auditing and/or certifying by Customer (or any independent or impartial inspection agents or auditors selected by Customer and not reasonably objected to by Caseware), with reasonable notice and during regular business hours. Before any information or audit is provided, the Parties shall mutually agree on the scope, timing, and duration of such audit.

17. Restricted Transfers

Any transfer of Personal Data from the EU or the EEA to a country outside the EU or the EEA that does not ensure an adequate level of protection as determined by decision of the EU Commission, will be subject to the Standard Contractual Clauses, at Attachment 3 and any transfer of Personal Data from the UK to a country that does not ensure an adequate level of protection as determined by decision of the EU Commission, will be subject to the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, at Attachment 4.

Customers transferring Personal Data from the EU or EEA or the UK to Caseware will be considered a "Data Exporter", and Caseware will be considered a "**Data Importer**" (both terms as defined in the Standard Contractual Clauses). Customer (as "**data exporter**") and Caseware (as "**data importer**") hereby enter into the Standard Contractual Clauses or the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as applicable, in respect of any Restricted Transfer from Customer to Caseware.

The Standard Contractual Clauses or the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as applicable, shall come into effect upon execution of the MPSA.

18. Liability

The liability of the Parties shall be subject to the liability provisions of the MPSA.

19. Term & Termination

This DPA becomes effective upon agreement with the MPSA and shall remain in force as long as Caseware processes Personal Data or throughout the term of the MPSA, whichever is longer.

20. Miscellaneous

In case of a conflict, between this DPA or any other agreement between the parties and the Standard Contractual Clauses, the Standard Contractual Clauses shall take precedence. In case of a conflict, between the provisions of this DPA and any other agreement between the Parties, this DPA shall take precedence. Should individual provisions of this DPA be or become invalid, this shall not affect the validity of the remaining conditions of this DPA. Without prejudice to Clause 17 (Governing Law) and Clause 18 (Forum and Jurisdiction) of the Standard Contractual Clauses, the Parties submit to the choice of jurisdiction and venue stipulated in the MPSA.

Attachment 1:

Technical and Organizational Measures (“TOMs”)

Action Description	Technical & Organizational Measures
Pseudonymization	Caseware employs tools to selectively anonymize sensitive data, which may include Personal Data. Pseudonymization is not necessarily used on all personal data elements, as not all Personal Data is identifiable as such to Caseware.
Encryption	Encryption is used for data at rest, and this encryption is provided by Amazon Web Services Inc. ("**AWS**"), an approved Sub- Processor (see **Attachment 2**). Digital certificates are in place to manage encrypted communications to the Amazon Web Servers.
Confidentiality	All Caseware Employees are required to sign a confidentiality agreement and accept company policies and procedures upon hire. An Information Security Incident Response Policy & Procedure is in place to address actual and potential data breaches.
Integrity	The Services provides administrative controls for clients to control who can access files within their firm. Caseware does not have these rights. Caseware is ISO 27001 and SOC 2 Type 2 certified, and controls are in place to ensure that only those required to perform administrative operations have required access. An access control policy and procedures are in place to review access control lists. Potential risks and the mitigation of potential risks are reviewed on a regular basis.
Availability	Monitoring is performed through an external health check and internally with capacity management monitoring solutions. Quality assurance processes are in place and under regular review, to mitigate against potential downtime.
Resilience of Processing Systems	The Services are hosted on AWS platform. The Service is ISO 27001 and SOC 2 Type 2 certified for security, confidentiality, integrity, privacy and availability.
Restoration	Backup Policy and procedures are in place, with daily automated backup reports to ensure restoration is achievable. Reports are monitored by an operational team.
Auditing/Testing	Regular audits take place for purposes of both ISO 27001 and SOC 2 Type 2 compliance. In addition, from time to time the company engages with a third party, for penetration testing services.

Certification(s)	ISO 27001 and SOC 2 Type 2.

Attachment 2:

Caseware's Sub-Processors

Sub-Processor	Purpose of Processing
Amazon Web Services Inc. 440 Terry Ave N. Seattle, WA 98108-1226, USA	Services and Subscriber Data is processed with Caseware licensed software, on Amazon Web Services Inc.'s infrastructure.
Amplitude 201 3rd Street, Suite 200 San Francisco, CA 94103, USA	A product analytics tool that allows Caseware's Product Management teams to better understand user behaviour. User actions across Caseware platforms are sent to Amplitude as "Events" along with properties on the user who performed that event. Low sensitivity data, accounting firm name and IP address are captured as user properties.
Google Analytics - Google Inc. 1600 Amphitheatre Pkwy. Mountain View, CA 94043, USA	A web analytics service offered by Google that tracks and reports website traffic that can help to identify trends and patterns in how visitors interact with Caseware's website.
Google Workspace - Google Inc. 1600 Amphitheatre Pkwy. Mountain View, CA 94043, USA	A collection of cloud computing, productivity and collaboration tools, software and products, to enable real-time collaboration between Caseware teams including, document creation, collection, and storage.
HubSpot 25 First Street, 2nd Floor Cambridge, MA 02141, USA	A customer relationship management (CRM) platform and marketing automation platform (MAP) for Caseware and its customers, prospects, and partners used by Caseware's Sales and Marketing team to communicate with customers.
Microsoft Dynamics GP Redmond, WA, USA	A cloud-based business platform that provides enterprise resource planning (ERP) services for Caseware's 'Back Office', invoicing and financial account management, inventory and supply chain management. Data collected, stored and processed is specific to fulfilling business services in performance of contracts.
NetSuite 2300 Oracle Way Austin, TX 78741, USA	A cloud-based business platform that provides enterprise resource planning (ERP) services for Caseware's 'Back Office', invoicing and financial account management, inventory and supply chain management. Data collected, stored and processed is specific to fulfilling business services in performance of contracts.
New Relic 188 Spear St #1000 San Francisco, CA 94105, USA	A log monitoring platform, technical service and Caseware application logs are sent to New Relic for search, analysis, and system monitoring. Sensitive data fields are masked such as usernames and emails, while some low sensitivity data such as IP and Host are captured directly.
Pendo.io Inc. 418 South Dawson Street Raleigh, NC 27601, USA	A product analytics tool that allows Cased Product Management teams to better understand user behaviour. User actions across Caseware platforms are sent to Pendo as "Events" along with properties on the user who performed that

	event. Low sensitivity data, accounting firm names are captured as user properties.
Salesforce Salesforce Tower 415 Mission Street, 3rd Floor San Francisco, CA 94105, USA	A customer relationship management (CRM) platform, for Caseware and its customers and partners. Used for marketing, leads and communication campaign management.
To The New (TTN) 2nd Floor, Wing - A, 2nd and 3rd Floor, Wing - B, Building No. 1, IT/ITES SEZ of M/s Golden Tower Infratech Private Limited Plot No. 08, Sector - 144 Noida, Uttar Pradesh 201301, India	TTN monitors the Services and provides 24x7 incident coordination support to ensure continued system availability to our clients. TTN escalates outages to Caseware’s internal Incident Response Team who then manage the lifecycle of the incident; investigation, remediation, and post-incident activities.

Attachment 3:

Standard Contractual Clauses

See attached.

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 -

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least annually. The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization.

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

> (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
>
> (ii) the data importer is in substantial or persistent breach of these Clauses; or
>
> (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

Defined terms used in this Annex 1 shall have the meaning given to them in the MPSA between Caseware and Customer, and/or the DPA.

A. LIST OF PARTIES

Data exporter(s):

1. Name: The data exporter is the legal entity specified as "Caseware" in the DPA

Address: Please see the DPA

Contact person's name, position and contact details: Please see the DPA

Activities relevant to the data transferred under these Clauses: Please see the DPA

Role (controller/processor): Processor

Data importer(s):

1. Name: The data importer is the legal entity specified as "Customer" in the DPA.

Address: Please see the DPA

Contact person's name, position and contact details: Please see the DPA

Activities relevant to the data transferred under these Clauses: Please see the DPA

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

- Please see the DPA, which describes the categories of data

Categories of personal data transferred:

- Please see the DPA, which describes the categories of data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- The parties do not anticipate the transfer of special categories of data.

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

- Please see the DPA

Nature of the processing

- Please see the DPA

Purpose(s) of the data transfer and further processing

- Please see the DPA

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

- Please see the DPA

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

- Please see the DPA

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

- The competent supervisory authority that shall apply will be the competent supervisory authority of the country in which the Customer's client's data originates

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Attachment 1 of the DPA, which describes the technical and organizational security measures implemented by Caseware.

ANNEX III

LIST OF SUB-PROCESSORS

See Attachment 3 of the DPA, which describes Caseware’s Sub-Processors.

Attachment 4:

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

See attached.

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

- Part 1: Tables
  - Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

- Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ **The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:** **Date:** **Reference (if any):** **Other identifier (if any):** **Or** ☐ **the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:**

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?

1						
2						
3						
4						

- Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Annex 1B: Description of Transfer:

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

- Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

- Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

- Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	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.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

- Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

- Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

    > "and, with respect to data transfers from controllers to processors and/or processors to

> processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

■ Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

- Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template 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 is revised under Section 18 of those Mandatory Clauses.