Data Processing Agreement

Effective Date: Effective Date of the Agreement.

RWS, and/or one of its Affiliates, (referred to as "RWS or Processor,") and Client (referred to as "Client or Controller") are parties to the Master Services Agreement (the "Agreement"). This Data Processing Agreement ("DPA") forms part of the Agreement and sets out supplemental provisions governing the processing of personal data during the provision of the Services.

In delivering the Services under the Agreement, RWS will process Personal Data as a data processor on behalf of Client, which is the data controller. The processing details (the duration, the nature, means and purpose of the processing, the types of personal data and categories of data subjects) are further specified in Exhibit 1 to the Agreement.

To the extent such processing is taking place, the relevant Data Protection Laws and this DPA will apply.

It is hereby agreed as follows:

1. Definitions.

1.1 All capitalized terms not specifically defined in this DPA shall have the same meaning as provided for in the Agreement. Terms used but not defined in this Section 1 (Definitions), such as "Personal Data" "Processing", "Controller", "Processor", "Data Subject" will have the same meaning as set forth in Article 4 of the GDPR.

1.2 The following definitions are used within this DPA:

"Affiliate" shall mean an entity (a) that directly or indirectly controls, is controlled by, or is under common control with a party under this Agreement, where "control" means ownership of more than fifty percent (50%) of the securities or voting power of the subject entity, and in the context of any other business entity, shall mean the right to exercise similar management and control of such entity, or (b) which is controlled, directly or indirectly, by the ultimate parent company, RWS Holdings Plc.

"Data Protection Laws" means applicable laws relating to the Processing of Personal Data (and any subsequent amendment, re-enactment, consolidation or replacement thereof):

i. As regards the Client so far as applicable to their collection and processing of the Personal Data; and

ii. As regards RWS in effect in the relevant jurisdiction where RWS's Processing of Personal Data as Processor for Client under the Agreement is to be carried out from time to time, including but not limited to the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR") and UK Data Protection Act 2018 ("UK DPA").

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

"Sub-processor" means any third party (including any Affiliate) engaged to process any Personal Data relating to this DPA and/or the Agreement.

2. Subject and Scope.

2.1 RWS shall process Personal Data under the Agreement only as a Processor acting on behalf of Client (whether the Client is a Controller or is itself a Processor on behalf of third party controllers). RWS agrees that it will process Personal Data in accordance with Client's documented instructions for the sole purpose of providing the Services as described in the Agreement(s) and Exhibit 1.

2.2 Client shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Client acquired Personal Data. Client's instructions for the Processing of personal Data shall comply with Data Protection Laws. Client is solely responsible for obtaining all necessary consents, licenses and approvals for the collection and Processing of any Personal Data. Client shall inform RWS accurately and without undue delay about the revocation of consent or any Data Subject request to access, correct or delete its Personal Data or if a Data Subject objects to the Processing thereof.

2.3 RWS and the Client shall comply with the Data Protection Laws applicable to it in connection with this DPA and shall not cause the other party to breach any of its obligations under Data Protection Laws.

2.4 Where the GDPR and or UK DPA apply RWS undertakes to comply with the provisions of GDPR Article 28 assisting the Client as required.

2.5 RWS will not sell the Personal Data. RWS is not permitted to collect, retain, use, or disclose Personal Data for its own purposes or for the purpose of any third party, firm, or enterprise (including Affiliates).

3. Technical, Organizational measures and Security.

3.1 RWS shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing the Personal Data. The parties agree that the security measures as described in **Exhibit A** are appropriate to protect Personal Data against a Personal Data Breach. That these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected having regard to the state of the art and the cost of their 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.

3.2 RWS shall ensure that any person authorized to process the Personal Data is subject to a strict duty of confidentiality and that they Process the Personal Data only for the purpose of delivering the Services under the Agreement.

3.3 At a minimum, RWS agrees to maintain a recognised standard of security either certified to ISO27001or SOC2 the scope of which contains the Security Measures identified at **Exhibit A**. The security measures will be reviewed on an annual basis and updated as RWS considers appropriate in order to protect the Personal Data against any new identified internal and external risks. RWS may modify its Security Measures from time to time and at any time, provided, however, that it will not materially reduce the level of protection as provided in this DPA.

3.4 RWS will maintain a Personal Data Breach Incident Response plan which will be reviewed annually.

4. Sub-processing.

4.1 RWS uses Sub-processors for the purposes of providing the Services to the Client as described in the Agreement. RWS currently uses the following categories of Sub-processors:

i. Freelancers

ii. Affiliates

iii. Providers of ancillary services such as telephony, IT services/applications which RWS uses in the ordinary course of business, including data centre hosting providers (detailed in the SaaS Privacy Policy located at https://www.rws.com/legal/privacy/hosted-products/

4.2 Client grants RWS general written authorization to engage with (i) the categories of Sub-processors in section 4.1; and (ii) new categories of Sub-processors provided that RWS gives Client reasonable prior notice. If Client objects on reasonable data protection grounds to the appointment of any new category of Sub-processor and RWS is unable to provide an alternative within a reasonable period of time, then Client may elect to suspend or terminate the Processing of Personal Data under the Agreements without penalty.

4.3 In any event RWS must (i) have executed a valid and enforceable written contract with the Sub-processor containing privacy and security provisions substantially similar to those contained in this DPA; (ii) RWS remains fully liable for any breach that is caused by an act, error or omission of such Sub-processor; (iii) have put in place appropriate measures to ensure that international transfers of Personal Data occur in compliance with applicable Data Protection Laws.

5. Cross-Border Transfers.

5.1 If the RWS contracting entity is located outside of the European Economic Area ("EEA") or UK the parties will execute the appropriate module of the Standard Contractual Clauses published in the European Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries dated 4 June 2021 ("SCC").

5.2 RWS will not process or transfer Personal Data outside of the EEA or UK unless:

i. it is to a country which is considered to ensure an adequate level of protection as determined by the EU or UK Government as appropriate;

ii. Or with respect to EU Personal Data, RWS has first entered into the Module 3 Processor to Sub-Processor of the SCC which are hereby incorporated into this

DPA Until 27 December 2022 RWS can rely upon the Standard Contractual Clauses for controllers annexed to European Commission Decision 2010/87/EU entered into prior to 27 September 2021. And with respect to UK Personal Data RWS has first entered into 1) the International Data Transfer Agreement ("IDTA") or 2) the International Data Transfer Addendum to the SCCs; which are hereby incorporated into this DPA.

5.3 In non-European countries or the UK which have regulations governing cross-border transfers RWS will comply with the appropriate regulations which apply to the RWS company.

5.4 The RWS Affiliate US companies and their Affiliates are registered under the EU-US Privacy Shield and/or Swiss-US Privacy Shield. The Processing by RWS's Affiliates in the USA will be under the appropriate SCC between RWS and its US Affiliate(s). The processing by RWS and RWS Affiliates in the USA will be under the Privacy Shield in accordance with the Privacy Shield Principles in addition to obligations under the SCC.

6. Deletion and Return.

6.1 Upon Client's written request, or upon termination of the Agreement, RWS will destroy subject to its customary data retention and archival processes all electronic Personal Data or return to Client all documented physical Personal Data in its possession or control. Upon RWS becoming aware of a dispute of whatsoever nature arising in respect of the performance or non-performance of the Services on request from RWS the Client shall within 5 business days provide copies of all the materials RWS returned to the Client. In any event Client shall provide copies of the original materials provided for translation and the original translated materials provided. In the event the original documents were not physical copies of the original documents but were electronic versions then copies provided will contain the metadata of the original versions provided. The Client agrees that such copies will be provided without the need for any official disclosure process to enable RWS to consider the allegations of any dispute for the purpose of resolving any issues without the need to resort to litigation. This requirement will not apply to the extent that RWS is required by any law governing RWS operations to retain some or all of the Personal Data, in which event RWS will securely isolate and protect the Personal Data from any further processing except to the extent required by such law.

7. Cooperation under GDPR and UK DPA.

7.1 To the extent RWS is required under GDPR and UK DPA, RWS will reasonably assist Client to comply with GDPR and UK DPA; in particular (i) RWS will assist Client in responding to any request from a Data Subject exercising his or her rights under the GDPR or UK DPA, RWS will not respond to that request except on the documented instructions of Client or as required by GDPR or UK DPA , in which case RWS shall to the extent permitted by GDPR or UK DPA inform the Client of that legal requirement before responding to that request; (ii) it will assist Client in responding to any request from regulatory or judicial bodies relating to the Processing of Personal Data under the Agreement; (iii) it will promptly notify Client if it believes that its Processing of Personal data is likely to result in a high risk to the privacy rights of Data Subjects; and (iv) upon reasonable request, will provide reasonably assistance to Client to carry out data protection impact assessments.

8. Personal Data Breach.

8.1 If RWS has reasonable grounds to believe that a Personal Data Breach may or has occurred in respect of the Personal Data being processed under the Agreement, RWS will inform Client without undue delay, and in any event within seventy-two (72) hours after becoming aware of such Personal Data Breach. In such event, RWS will (i) provide reasonable information and cooperation to Client so that Client can fulfil any Personal Data Breach reporting obligations it may have; (ii)take appropriate measures to mitigate the effects of the Personal Data Breach; (iii) keep Client informed of all material developments with the Personal Data Breach; and (iv) co-operate reasonably with the Client in relation to any investigation that Client may initiate, or which may be initiated by a Supervisory Authority.

9. Security Reports and Audits/Inspections.

9.1 RWS shall maintain records in accordance with its ISO 27001 or SOC 2 certification statement or similar Information Security Management System ("ISMS") standards. Upon request, RWS shall provide copies of relevant external ISMS certifications, independent audit report summaries and/or other documentation reasonably required by Client to verify RWS's compliance with this DPA. Such documentation will be subject to the confidentiality provisions under the Agreement.

9.2 RWS will allow the Client on at least thirty (30) days written notice to audit RWS's compliance with this DPA. Such audits will take place during RWS business hours and will be limited to one in any twelve-month period but in the event of a Personal Data Breach an additional audit may be performed. The parties will agree in advance on reasonable timing, scope, and security controls applicable to the audit (including restricting access to RWS's trade secrets and data belonging to RWS's other customers).

10. General.

10.1 The obligations placed under this DPA shall survive so long as RWS and/or its Sub-processors processes Personal Data on behalf of Client.

10.2 RWS will have the right to amend this DPA provided that RWS does not reduce the level of its obligations in the DPA.

10.3 If any part of this DPA is held unenforceable, the validity of all remaining clauses will not be affected.

10.4 In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall prevail.

10.5 RWS shall appoint a data protection officer where required by the Data Protection Laws, and where a data protection officer is not required RWS will have a Data Privacy Officer responsible for data protection. All data protection matters are to be raised with the RWS Data Privacy Officer at privacy@rws.com.

10.6 Notwithstanding anything stated elsewhere in this DPA, liability under this DPA shall be capped as under the Agreement.

10.7 This DPA shall be governed by the laws of the Agreement.

Exhibit A

Technical and Organizational Security Measures

This Exhibit A sets out a description of the technical and organizational security measures that RWS will implement and maintain throughout the provision of Services.

Access Control to Processing Areas and Data Processing Systems

Implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are processed or used and processing systems. This is accomplished by:

- Using dedicated datacenter facilities for housing data.
- Maintaining a high standard of physical security in all facilities i.e. swipe card access, on site guards, locked doors between different parts of the building, zone level access control.
- Ensuring that applications are logically separated in their deployed tiers.
- Ensure that all employees authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality for the duration of their employment, as well as after termination of their employment. The parties shall also ensure that employees observe the data secrecy provisions prior to taking up their duties and are familiar with the data protection legislation and rules relevant to them.
- Maintaining an active information security programme which includes ISO 27001 certification and standards.
- Internal and external audit programmes.
- Security testing both as part of the security but also vulnerability scanning within the operational environment.

Regular patching and software updates are applied as required.

Access Control to Use Specific Areas of Data Processing Systems

- Commit that the persons entitled to use the data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied, modified or removed without authorization. This shall be accomplished by:
- Appropriate access control is maintained to the systems and personal data is highly protected in line with industry standard data classification and treatment policies. Employees who have elevated level of access are required to undertake mandatory information security awareness training.

- All users are required to use named accounts and access to systems and data is logged.

Transmission Control

- Implement suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:
- Personal Data is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys or is transferred over private network connectivity.

Input Control

- Implement suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This is accomplished by:
- Utilization of user identification credentials, authentication of the authorized personnel, session time outs etc.

Job Control

- Ensure that personal data may only be processed lawfully. This is accomplished by:
- Adherence to the instructions provided for processing, training of staff to maintain awareness of security and privacy requirements, maintenance of logs and auditing activity.

Availability Control

- Implement suitable measures to ensure that personal data is protected from accidental destruction or loss. This is accomplished by:
- Global and redundant service infrastructure, resilient backup technology and processes in place to test our capability to restore data.

Separation of processing for different purposes

- Implement suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:
- Determining defined processing paths to ensure workflow capability and required processing steps of different data is controlled.

Personal Data Breach

- Implement suitable measures to ensure that personal data breaches will be handled in accordance with the Applicable Law and in collaboration by both parties. If a personal data breach arises Applicable law will be complied with in determining how to respond in particular with respect to notice to competent any supervisory authority and to data subjects.

Data Subject Rights

- Implement suitable measures to ensure that data subject can enforce their rights.