DATA PROCESSING AGREEMENT

For Suppliers

(Controller to Processor or Processor to Sub-Processor)

This Data Processing Agreement and all of its Exhibits ("DPA") sets forth obligations of RWS, on behalf of itself and Affiliates (collectively "RWS") and Supplier in relation to personal data processing activities performed by Supplier on behalf of RWS under the agreement(s) pursuant to which Supplier provides services to RWS (together "Main Agreement(s)") which this DPA forms an integral part of.

In the event of any conflict or inconsistency between the provisions of this DPA and the provisions of a Main Agreement, the provisions of the DPA shall prevail.

All capitalized terms not defined herein shall have the meaning set forth in the Main Agreement.

1. DEFINITIONS

1.1 **Affiliate** means 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;

1.2 **Data Controller** means the entity responsible for determining the purposes and the means of personal data processing activities as per the definition given under the European Union General Data Protection Regulation (EU GDPR) and/or local equivalent data protection laws and regulations;

1.3 **Data Processor** means the entity processing personal data on behalf of the Data Controller as per the definition given under the EU GDPR and/or local equivalent data protection laws and regulations;

1.4 **Data Protection Impact Assessment (DPIA)** means a comprehensive analysis of processing of Personal Data to identify and mitigate data protection risks;

1.5 **Data Protection Laws** means applicable data protection legislations and regulations including, but not limited to, the EU GDPR (Regulation (EU) 2016/679), and their local equivalent around the globe;

1.6 **Data Subject** means the individuals whose personal data is processed by Supplier under this DPA;

1.7 **European Economic Area (EEA)** means an economic region that links Iceland, Norway and Liechtenstein to the European Union (EU);

1.8 **EU SCCs** means the standard contractual clauses set out in the Annex of Commission implementing decision (EU) 2021/914 of 4 June 2021. The text of the EU SCCs incorporated to this DPA by reference shall be applied "as is", except (i) selecting applicable modules and/or specific options offered in the text, (ii) completing the text where necessary, e.g. to indicate the competent courts and supervisory authority, and to specify time periods, (iii) filling in the Annexes or (iv) addition of additional safeguards that increase the level of protection for the Personal Data. These adaptations are not considered as altering the core text;

1.9 **Instructions** means RWS documented instructions to Supplier, which may be specific instructions or instructions of a general nature as set out in the Main Agreement or DPA or as otherwise notified by RWS to Supplier during the term of the Main Agreement and relating to the processing of personal data;

1.10 **Personal Data** means any information relating to an identified or identifiable natural person defined under the Data Protection Laws and that Supplier processes on behalf of RWS as Data Controller or as Data Processor;

1.11 **Personal Data Incident(s)** means an actual or suspected breach of security relating to Personal Data in Supplier's systems, facilities or equipment and/or Supplier's sub-contractors' systems, facilities or equipment and leading to (i) accidental or unlawful destruction, loss, damage and/or alteration of Personal Data; (ii) unauthorised disclosure and/or access of Personal Data; and/or (iii) any and all other unauthorised or unlawful forms of processing upon Personal Data;

1.12 **Processing, Process and Processed** means one or more of the following activities: collection; recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, destruction performed on the Personal Data;

1.13 **Security Policy** means the minimum security requirements to be applied by Supplier when Processing Personal Data to fulfil the services described under the Main Agreement;

1.14 **Sub-Processor** means any third party or where applicable a Supplier Affiliate involved directly or indirectly in the provision of the Services where Personal Data is Processed pursuant to the Main Agreement and any applicable order form, statement of work, quotation or other ordering document (each referred to herein as Order Form);

1.15 **Third Country** means any country outside the UK and/or European Economic Area (EEA), not benefiting from an adequacy decision pursuant to the GDPR;

1.16 **Transfer Impact Assessment (TIA)** means an assessment of the privacy protections of the laws and regulations of a recipient country outside of the EU/EEA;

1.17 **UK Addendum** means International Data Transfer Addendum to the EU SCCs.

1.18 **Whole Agreement** means the Main Agreement, DPA, Exhibits and any other ancillary document comprising the contract.

2. GENERAL PROCESSING TERMS

2.1 Purpose Limitation

2.1.1 The Parties agree that Supplier is providing Services as defined in the Main Agreement, acting as Processor or Sub-Processor as the case may be (as mentioned in Exhibit 1) to RWS, acting accordingly as Controller or Processor.

2.1.2 Supplier shall carry out the Processing of Personal Data under RWS Instructions solely for the purposes necessary for the fulfilment of the Services described under Main Agreement and any Order Form from time to time, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which

Supplier is subject; in such a case, Supplier shall inform RWS of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.1.3 Supplier shall immediately inform RWS if, in its opinion, an Instruction infringes Data Protection Laws.

2.1.4 Supplier (i) shall not Process Personal Data for its own purposes, such as improving its products, performing research and development, disclosing to a third party for commercial benefit to Supplier or any third party, or for any other business purpose; (ii) shall not combine Personal Data with personal information Supplier receives from, or on behalf of, other persons, or collects from its own interactions with an individual; (iii) shall not use Personal Data to train any artificial intelligence or machine learning engine or system, neural network, or similar system, absent a separate executed agreement with RWS expressly permitting these activities; and (iv) shall not use Personal Data for marketing or advertising purposes, nor sell Personal Data as per the meaning of Data Protection Laws.

2.1.5 The subject matter and description of the Processing of Personal Data by Supplier is detailed under the Main Agreement or Order Form.

2.2 Confidentiality

Supplier shall ensure that all personnel of Supplier and Supplier Sub-Processors who are authorized to access Personal Data (Authorized Personnel) are expressly bound by confidentiality obligations at least as strict as those contained in the Main Agreement. Supplier shall only permit access to Personal Data by Authorized Personnel on a need-to-know basis to the extent required for the performance of the specified purposes of the Processing, and Supplier shall ensure that all Authorized Personnel have received appropriate privacy and security training, which shall be updated periodically in accordance with Data Protection Laws.

2.3 DPIA

Upon request, Supplier shall assist RWS in performing any DPIA.

2.4 Infringement

Supplier will notify RWS without undue delay in writing if Supplier or a Supplier Sub-Processors makes a determination that it can no longer comply with its obligations under Data Protection Laws. Following such notice, RWS has the right, upon providing notice to Supplier, to take reasonable and appropriate steps to stop or remediate any Processing of Personal Data infringing Data Protection Laws. Supplier will reasonably cooperate with RWS in curing any alleged violation of Supplier's obligations under Data Protection Laws. Upon request, Supplier will provide RWS with a written statement confirming such cure.

2.5 Compliance

Supplier shall Process Personal Data in compliance with all Data Protection Laws, this DPA and Exhibits, and the Main Agreement.

3. ASSISTANCE AND COOPERATION

3.1 Supplier shall assist RWS in ensuring compliance with its obligations relating to Supplier's Processing of Personal Data under the Main Agreement as required under Data Protection Laws.

3.2 At RWS request, Supplier shall provide without delay all necessary assistance by appropriate technical and organisational measures to fulfil RWS obligation to respond to any request or inquiry RWS may receive from a Data Subject, data protection supervisory authority or regulatory body, law enforcement agency or government in relation to the Processing of Personal Data.

3.3 Supplier shall also immediately inform RWS in writing of any request, inquiry or complaint by a Data Subject, data protection supervisory authority or regulatory body, law enforcement agency or government that it may directly receive in relation to the Processing of Personal Data.

3.4 Supplier shall not disclose or report any information to any Data Subject, data protection supervisory authority or regulatory body, law enforcement agency or government in relation to the Processing of Personal Data without the prior written consent of RWS unless notification to RWS is prohibited by applicable law.

3.5 RWS shall be informed in writing, including email, without undue delay of any change of the data protection officer or direct point of contact for all privacy matter.

a. RWS contact details: as defined in the Main Agreement

b. Supplier's data protection officer, or, if not applicable, direct point of contact for any privacy matter: as defined in the Main Agreement

4. DATA SECURITY

4.1 Security Measures

4.1.1 Supplier shall take all administrative, technical and organizational measures required, including but not limited to the minimum requirements described under Exhibit 2, to ensure at all times the confidentiality, integrity, availability and resilience of Supplier systems, Processes and procedures that involve the Processing of Personal Data.

4.1.2 Supplier shall protect Personal Data against (i) accidental and/or unlawful destruction, loss, damage and/or alteration; (ii) unauthorised disclosure and/or access; and/or (iii) any and all other unauthorised or unlawful forms of Processing.

4.1.3 Throughout the term of the Agreement, Supplier will maintain and monitor a comprehensive, written privacy and information security program, including policies and procedures, that contain administrative, technical and physical safeguards designed to protect against anticipated threats to the confidentiality, integrity, availability or resilience, and the unauthorised Processing of, Personal Data. Supplier will periodically assess foreseeable risks to the confidentiality, integrity, availability or resilience of electronic, paper and other records containing Personal Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks.

4.1.4 Upon RWS request, Supplier shall provide information about its privacy and information security program.

4.2 Personal Data Incident

4.2.1 Supplier shall have in place a dedicated program to manage and mitigate the consequences of Personal Data Incidents as defined under this DPA.

4.2.2 Upon the occurrence of a Personal Data Incident, Supplier shall:

a. notify RWS of the Personal Data Incident by submitting written information via email to RWS supplierincident@rws.com within 24 hours, such notification to include a detailed description of the Personal Data Incident with the information set forth in Exhibit 3;
b. take immediate steps to contain the Personal Data Incident and mitigate its consequences, including, without prejudice to any other rights or remedies of RWS under this DPA, at law or otherwise, restore to the last available back-up of any Personal Data that may have been lost, damaged or destroyed as a result of the Personal Data Incident;
c. investigate the Personal Data Incident
d. assess the risks and potential adverse consequences associated with the Personal Data Incident;
e. collaborate closely and without delay with RWS to determine the appropriate responses and actions, including where applicable, notifications to the relevant Data Subjects and any other external disclosures;
f. assist RWS upon request with the carrying out of all remedial measures including providing credit monitoring services to affected Data Subjects at Supplier's expense and associated with the management and mitigation of the Personal Data Incident as determined by RWS or required under any law.

4.2.3 Supplier shall document the Personal Data Incident, including the facts relating to the Personal Data Incident, its effects and the remedial actions taken, and Supplier shall make available that documentation to RWS.

4.2.4 Unless otherwise required by Data Protection Laws or other law, rule, regulation or order, Supplier shall not report any Personal Data Incident to any Data Subjects, data protection supervisory authority, regulatory body, law enforcement agency or government without RWS prior written consent.

5. LIABILITY AND INDEMNITY

Supplier shall be liable for, indemnify, defend and hold RWS harmless from and against any and all losses (including Personal Data losses and corruptions), penalties, fines (including administrative fines which may be pronounced by any data protection supervisory authority or regulatory body), costs, expenses, damages, (whether direct, indirect or consequential, loss of profit, loss of reputation and all interest, legal and other reasonable professional costs) incurred by RWS as a result of:

a. a Personal Data Incident as defined in this DPA;
b. claims made by third parties (including, without limitation, RWS clients and Data Subjects) in relation to Supplier's acts or omissions under this DPA; and/or
c. any breach of Data Protection Laws by Supplier or any of its Sub-Processors, and any Supplier's failure to comply with its representations, warranties and/or obligations under this DPA.

Notwithstanding any conflict with the order of precedence of the legal documents comprising the Whole Agreement, this liability and indemnity obligation shall not be subject to any exclusion or limitation of liability provisions in the Main Agreement.

6. INTERNATIONAL TRANSFERS OF PERSONAL DATA

6.1 To the extent any personal data originating from the European Economic Area (EEA) or the UK countries is transferred to countries outside of the EEA/UK that have not been deemed to have adequate data privacy laws in place, the EU SCCs also known as EU Model Clauses and with respect to UK personal data, the UK Addendum are hereby incorporated by reference.

Supplier shall also document any required Transfer Impact Assessment as per the applicable regulatory guidelines and make the same available to RWS upon request.

6.2 EU SCCs

Where EU SCCs apply, they will be deemed completed as follows:

i. Module 1 (Controller to Controller) will apply when RWS Processes the Personal Data as a Data Controller. Then RWS acting as Data Exporter, transfers Personal Data to Supplier, acting as a Data Importer, which will also be a Data Controller of the Personal Data transferred. An example of a situation when this Module will apply is in respect of RWS' staff contact data which is provided to the Supplier for the purposes of the business relationship between the parties.

ii. Module 2 (Controller to Processor) will apply when Supplier processes the Personal Data as a Data Processor on behalf of RWS as a Data Controller. Then RWS acting as a Data Exporter will transfer the personal data to Supplier. Supplier acting as a Data Importer will be a processor of the personal data transferred.

iii. Module 3 (Processor to sub-Processor) will apply when Supplier Processes the Personal Data as a Data Processor on behalf of third party as a Data Controller. Then RWS acting as a Data Exporter will transfer the Personal Data to Supplier. Supplier acting as a Data Importer will be a sub-processor of the Personal Data transferred.

iv. in Clause 7, the optional docking clause will not apply;

v. in Clause 9(a), Option 1 "Specific Prior Authorisation" will apply, and the time period for prior notice of Sub- processor changes shall be as set out in Section 6 of this DPA;

vi. in Clause 11, the optional language will not apply;

vii. in Clause 17, Option 1 will apply and will be governed by the laws provided in the Main Agreement. If the Main Agreement is not governed by an EEA member state law, then the laws of Ireland shall govern;

viii. in Clause 18(b), disputes shall be resolved before the courts provided in the Main Agreement. If the Main Agreement does not provide courts in an EEA Member State, the parties agree to the courts of Dublin;

ix. Annex I.A and I.B and Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit 1 and Exhibit 2 to this DPA;

x. Annex III of the EU SCCs shall be deemed completed with the information set out in Exhibit 4 to this DPA and;

xi. in Annex I.C of the EU SCCs, where the data exporter is established in the EEA, the Supervisory Authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer shall be the Authority of the member state in which the data exporter is established. Where the data exporter is not established in the

EEA, but is within the territorial scope of application of GDPR in accordance with Article 3(2) and has appointed a representative pursuant to Article 27(1), the Supervisory Authority shall be the member state in which the representative within the meaning of Article 27(1) is established. If the data exporter is not established in the EEA, but falls within the territorial scope of application of GDPR without having to appoint a representative pursuant to Article 27(2), the Supervisory Authority of Ireland shall act as the competent Supervisory Authority.

Nothing in the interpretations in this Section 5.2 is intended to conflict with either Party's rights or responsibilities under the EU SCCs and, in the event of any such conflict, the EU SCCs shall prevail.

6.3 UK Addendum

Where the UK Addendum applies, it will be deemed completed as follows:

i. Table 1 shall be deemed completed with the information set out in Exhibit 1 of this DPA, the contents of which are hereby agreed by the Parties;
ii. Table 2, the Parties select the checkbox that reads: "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", and the accompanying table shall be deemed completed according to the Parties' preferences outlined in Section 5.2 above;
iii. Table 3, shall be deemed completed with the information set out in Exhibit 1 and Exhibit 2 and Section 6 of this DPA; and
iv. Table 4, the Parties agree that neither Party may terminate the UK Addendum as set out in Section 19.

7. SUB-PROCESSORS AND THIRD PARTIES

7.1 Supplier shall not sub-contract any of its processing activities performed on behalf of RWS under this DPA to a Sub-Processor without RWS's prior specific written authorisation. Supplier shall submit the request for specific authorisation at least 30 days prior to the engagement of the Sub-Processor, together with the information necessary to enable RWS to decide on the authorisation. The list of Sub-Processors already authorised by the data exporter can be found in Exhibit 4. The Parties shall keep Exhibit 4 up to date.

7.2 Except as per 6.1 above, Supplier shall not engage, in the context of the provision of the services under the Main Agreement, any Sub-Contractor without RWS prior specific written authorization, to be sought at least 30 days in advance.

7.3 Any Sub-Contractor engaged by Supplier shall be contractually bound by way of a written contract that provides for data confidentiality, privacy and security obligations at least as strict as those binding Supplier under the Main Agreement and this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Laws. RWS shall have the express right to review and audit upon 24 hours' notice the agreement and any subsequent amendments concluded between Supplier and its Sub-Contractors. Supplier shall promptly implement changes requested by RWS and necessary in its reasonable opinion to ensure compliance with this DPA and Data Protection Laws.

7.4 If a Supplier Sub-Contractor Processes Personal Data in a Third Country, Supplier shall ensure compliance with Data Protection Laws by applying appropriate measures, including without limitation the execution of the EU SCCs or any other alternative as prescribed by Data Protection Laws. Should these EU SCCs or other chosen alternative in the future be declared null and void and/or be revised by a relevant data protection authority, including the European Commission, Supplier will without undue delay, apply the then applicable and/or available instruments required to provide for appropriate safeguards required for the Third Country transfers and enter into such agreed instruments in a written and legally binding form with its Supplier Sub-contractors.

7.5 In any event, Supplier shall remain fully liable for all acts and omissions and failure to fulfil data protection obligations of its Sub-Contractors with respect to the Personal Data processed including Personal Data Incidents and any breach of Data Protection Laws.

8. DELETION OF PERSONAL DATA

Upon termination of this DPA or the Main Agreement or after the end of provision of Services, or sooner at RWS request, Supplier will promptly delete any Personal Data and all copies thereof. Supplier shall provide, upon RWS request, a certificate of destruction signed by an authorized director of Supplier certifying compliance with this provision.

9. RECORDS AND AUDITS

9.1 Records

9.1.1 The Supplier shall keep and maintain (and where applicable shall require its Sub-Contractors keep and maintain) during this DPA and for the applicable local retention period after its termination or expiry, complete and accurate records of Processing activities performed on behalf of RWS as per Data Protection Laws as well as of records of any Personal Data Incident that occurred during the term of the Main Agreement.

9.1.2 Supplier shall expressly allow (and shall require its Sub-Processors to allow) RWS during this Agreement and for seven years after its termination or expiry, to access, inspect, audit and, in respect of electronic or paper documents, take copies of the above-mentioned records during normal business hours provided the RWS has given Supplier a five-calendar day prior written notice. Supplier shall make available to RWS all information necessary to demonstrate compliance with the obligations laid down in Data Protection Laws.

9.2 Audit

9.2.1 In addition to RWS rights set forth in the Security Policy referred to in this DPA, RWS shall have upon prior written notice of five calendar days the right to carry out no more than once in any 12 (twelve) consecutive months an audit of all Supplier information necessary to demonstrate compliance with this DPA and its exhibits. RWS may conduct the audit directly or via an independent auditor, at its sole discretion. Supplier shall provide RWS all required assistance. Each party will pay for its own related costs, except where the audit results in non-compliance, in which case Supplier shall reimburse RWS for its costs.

9.2.2 When conducting audits, RWS shall comply with Supplier's reasonable directions in order to minimise disruption to Supplier's business and to safeguard the confidentiality of Supplier's other confidential information.

9.3 Audit Findings

9.3.1 Where an audit, whether performed by Supplier or RWS, reveals a data security risk and/or privacy compliance risk that may impact the protection of Personal Data, or reveals a Personal Data Incident, breach or non-compliance of this DPA and/or Data Protection Laws, Supplier shall immediately develop rectification steps under a remediation project plan.

9.3.2 Such plan shall be submitted to RWS within 5 calendar days, any extension to be submitted to RWS for approval, and RWS shall have the right to request any reasonable further rectification steps. Written evidence of remediation shall be provided to RWS upon request.

9.3.3 In the event that Supplier has not remedied the risk, RWS shall be entitled to terminate this DPA and the Whole Agreement with immediate effect. Supplier shall not be entitled to any compensation or damages as a result of such termination. Such termination shall be without prejudice to any damages or other remedies RWS may be entitled to.

10. GENERAL NOTIFICATIONS

All notices or other communications to a party required or permitted hereunder shall as described under this DPA or be in writing and shall be delivered in person, sent by a nationally recognized express delivery service which tracks delivery, or sent by certified/registered mail, postage prepaid with return receipt requested, to the address indicated on the first page of this DPA, or such other address provided by such party in writing. Either party may change its address for notices under this DPA by giving written notice to the other party by the means specified in this Section.

11. MISCELLANEOUS

In the event that any provision of this DPA is held by a court or other tribunal of competent jurisdiction to be unenforceable, the remaining provisions of this DPA shall not be affected and shall remain in full force and effect. The failure or delay by a party to enforce its rights hereunder shall not be deemed a subsequent waiver of that right or to waive enforcement of any other term or right. This DPA may not be amended or modified except by a writing signed by both Parties hereto. The headings of the sections of this DPA are inserted for convenience only and shall not be deemed to constitute a part of this DPA.

EXHIBIT 1 – DESCRIPTION OF THE PERSONAL DATA PROCESSING / TRANSFER

Data exporter: RWS
Name, address and contact details: Provided in the Main Agreement.
Activities relevant to the data transferred under these Clauses: Provided in the Main Agreement.
Signature and date: Provided in the Main Agreement.
Data exporter's role: ☐ RWS is Data Controller/ ☐ RWS is Data Processor

Data importer: Supplier
Name, address and contact details: Provided in the Main Agreement.
Activities relevant to the data transferred under these Clauses: Provided in the Main Agreement.
Signature and date: Provided in the Main Agreement.
Data importer's role: ☐ Supplier is a Data Processor/ ☐ Supplier is Data Sub-Processor

In the event that Personal Data is not transferred outside of the jurisdiction of collection, then the Table below should be read as data processed not transferred. The table below will be filled out as part of the applicable Order Form.

Category	**Description**	
Categories of data subjects whose personal data is transferred	RWS employees	☐
	RWS's Contractors, consultants, freelancers, contingent workers and/or temporary agency workers	☐
	Potential personnel of RWS, including job applicants/candidates	☐
	General public	☐
	Other – please specify: _____	☐
Categories of personal data transferred	Name	☐
	Other personal details about the data subject (such as gender, date of birth, place of birth or nationality)	☐
	Personal details issued by a public authority (such as passport, driver's license or social security number)	☐
	Contact information (such as address, phone number or e-mail address)	☐
	Education, qualification or training details	☐
	Employment details	☐
	Financial details	☐
	Other – please specify: _____	☐
Sensitive data transferred (if applicable) and applied	All categories below	☐
	None of the categories below	☐

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	Personal data regarding racial or ethnic origin	☐
	Personal data regarding political opinions	☐
	Personal data regarding religious or philosophical beliefs	☐
	Personal data regarding trade union membership	☐
	Genetic data and biometric data (such as fingerprint and retinal scan)	☐
	Data concerning health	☐
	Data concerning a natural person's sex life or sexual orientation	☐
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis ☐ or One-off basis ☐		
Nature of the processing *And purpose(s) of the data transfer and further processing*	The performance of such operations as may be necessary to carry out the RWS's (as data exporter) instructions in connection with the Services provided by Supplier (as data importer). Such processing operations may include, but are not limited to, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, as required by RWS to enable (check all that apply): Supplier to provide the Services and/or any deliverables ☐ Supplier to provide benefits to RWS personnel ☐ Supplier to provide the Services and/or any deliverables to RWS client(s) ☐ Other – please specify: _____ ☐	
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period		
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Describe the specific technical and organisational 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: If the Data Importer is authorised to engage sub-processors then the applicable technical and organisational measures are the security	

	requirements set out in the Exhibit 2 of the DPA between the Data Exporter and Data Importer which the sub-processor must adopt.

EXHIBIT 2 – SECURITY POLICY

This Security Policy describes the minimum security and data privacy obligations that are to be met by Supplier when Processing Personal Data for the fulfilment of the Services described under the Main Agreement. These obligations are without prejudice to the Supplier's other obligations set out in the Main Agreement.

All capitalized terms not defined herein shall have the meaning set forth in the Main Agreement or DPA.

1. LIABILITY

The Supplier expressly accepts liability for ensuring that the obligations described hereunder are fulfilled when Processing Personal Data either directly or indirectly by its Sub-Processors and/or third-party contractors (together referred to as Supplier).

2. BINDING POLICIES AND PROCEDURES

Supplier shall document its own binding security and privacy policies and procedures ("Security Documentation") in compliance with applicable Data Protection Laws including the security obligations described in this Security Policy in relation to the provision of the Services; such documentation shall be kept up to date by Supplier on an annual basis.

The Security Documentation shall clearly identify the physical, technical and organizational measures implemented by Supplier to adequately protect the Personal Data notably from unauthorized access, acquisition, use, disclosure, or destruction. Suppliers shall, on request, provide RWS with copies of the Security Documentation.

3. INFORMATION SECURITY PROGRAM

The Supplier shall implement and maintain an information security program, suite of policies and organisational structure with defined roles and responsibilities and shall appoint an Executive Sponsor responsible for overseeing the implementation and maintenance of the aforementioned information security program; The Executive Sponsor shall have the authority to allocate resources and make decisions necessary to ensure the security of personal data processed under this Agreement and shall report directly to the senior management of the Supplier. The Supplier shall regularly review the performance of and update the information security program to address new threats, vulnerabilities, and all applicable regulatory requirements.

4. RISK MANAGEMENT

The Supplier shall conduct periodic independent security risk evaluations to identify the criticality of information assets, assess threats to such assets, determine potential risks, and implement an appropriate and corresponding risk treatment plan. The Supplier shall implement appropriate technical and organizational measures to mitigate identified risks, ensuring a level of security appropriate to the risk.

5. INVENTORY

Suppliers shall maintain an inventory to ensure traceability of media, servers, and equipment containing Personal Data. This inventory shall document the return or destruction of Personal Data.

6. PERSONNEL

Supplier shall establish a background check process for Supplier personnel who have access to RWS Personal Data. This process shall include a criminal background check, employment verification, and reference checks as permissible under local laws and regulations.

Supplier shall require all Supplier personnel to sign an NDA or confidentiality agreement which outlines their responsibilities for protecting Personal Data and the consequences of non-compliance.

Supplier shall provide on an annual basis information security and data protection awareness, education and training for its personnel and any relevant Sub-Processors should the case arise.

7. USER AUTHENTICATION

Supplier access to information systems processing Personal Data is conditional upon implementation and completion of authentication procedures.

Supplier shall implement user authentication policies that require a unique login account for each user and user password policy that complies with regulatory recommendations, industry standards and best practices. At a minimum, passwords shall be at least 14 characters in length and include a combination of uppercase and lowercase letters, numbers, and special characters, and at least one additional factor, such as biometric recognition, passphrases, PINs, One Time Passcode (OTP). Passwords shall be changed at least every 90 days and not reused. Passwords shall not be disclosed to anyone else or written down at any time.

Supplier shall require users change any password assigned automatically or by an administrator and limit the number of attempts to access an account.

8. LOGICAL ACCESS

Supplier shall implement strict access privileges policies that require pre-defined profiles for access rights typically based on job requirements, removal of outdated access permissions and an annual review of access rights. Authorisation to access information systems processing Personal Data shall be restricted on a need-to-know basis so that only authorised users shall have access to the Personal Data strictly necessary for them to perform their duties.

The Supplier shall implement separation of duties controls to ensure that personnel with privileged access do not also have access to other sensitive systems or data. The Supplier shall also implement rotation of duties controls to ensure that no single individual has continuous access to privileged systems or data.

9. ENCRYPTION, HASHING AND SIGNING

Supplier shall use recognized and secure algorithms, software and libraries and keep secrets and cryptographic keys secure. Supplier shall protect all Personal Data in the Supplier infrastructure and environment equally regardless of the classification of the type of Personal Data as it is in transmission or at rest, using controls including, but not limited to:

- The encryption algorithm used shall be strong enough to prevent unauthorized access to Personal Data and based on industry best practice, such as: Advanced Encryption Standard (AES);
- The encryption key used to encrypt Personal Data shall be managed securely. It shall be generated randomly and be of sufficient length to prevent brute force attacks. Key management practices shall also include the secure rotation and destruction of keys;

- Personal Data shall be transmitted securely, using secure communication protocols such as Transport Layer Security (TLS);
- To prevent unauthorized access to the Personal Data shall be encrypted when at rest, using the above stated encryption algorithms and secure key management practices;
- The encryption methodology used shall comply with applicable regulations;
- Supplier shall encrypt Personal Data before sending to authorized external parties, ensure Personal Data is shared with the correct recipient and transmit the secret in a separate dispatch and through a different channel.

10. LOGGING

Supplier shall maintain appropriate audit trails of access or system logs to Information System(s) processing Personal Data to prevent tampering and anomalies by a trained security team. Audit logs shall be able to reasonably determine the applications/files accessed, user ID of the individual accessing the applications/files, the date, time and type (e.g. remote, local etc.) of access, and whether access was authorized or denied.

Application level and user access logs shall be made available to RWS upon request.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

The Supplier shall implement physical and environmental security measures to prevent unauthorized physical access, damage, and interference to the data and information provided by RWS, including but not limited to:

- Supplier shall establish physical access controls to limit access to RWS's data and information to authorized personnel only. Examples of suitable access controls include physical barriers such as locked doors and gates, security guards, access cards and biometric identification systems;
- Supplier shall implement environmental controls to protect RWS's data and information from environmental threats such as fire, flood, and temperature fluctuations. Environmental controls will include fire suppression systems, water detection systems, temperature and humidity controls, and backup power supplies;
- Supplier shall implement asset management controls to track the location and status of all equipment, hardware, and software that stores or processes Personal Data and information. Asset management controls will include inventory management systems, labelling and tagging systems, and regular physical inspections;
- Supplier shall establish secure work areas where personnel can access Personal Data and information without the risk of unauthorized access or theft. Secure work areas will include locked cabinets and rooms, surveillance cameras, and restricted access controls;
    - Supplier shall establish and maintain policies and procedures for physical security that are in line with industry standards. The policies and procedures will cover topics such as access controls, environmental controls, asset management, secure work areas, and incident response;
    - Supplier shall implement monitoring procedures to ensure that physical security controls are functioning as intended. Monitoring procedures will include regular inspections, audits, and testing of physical security controls;

- Supplier shall apply industry standard destruction of sensitive materials before disposition of media, securely store damaged hard disks prior to physical destruction and physically destroy all decommissioned hard disks storing data;
- As applicable, Supplier shall ensure physical access restrictions to its Data Center facilities and monitoring of the same that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (for example, fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; Supplier shall ensure equipment and/or media used for processing Personal Data shall be protected from physical and environmental threats to prevent interruption to the Supplier's activities and/or loss of Personal Data. Equipment and/or media containing Personal Data shall be locked away when not in use to prevent unauthorised physical access, damage, and interference to the information;
- Where hard copy records containing Personal Data are to be retained in manual filing systems, they shall be stored and filed according to appropriate criteria which enable the Supplier to locate the relevant records where necessary to facilitate the access, amendment or destruction of the relevant records, and the exercise of data subject rights at the request of RWS or the Data Subject to whom those records relate;
- Containers with locks or equivalent devices to prevent tampering and/or unauthorised access shall be used to store or transport hard copy records. Hard copy records containing Personal Data shall be securely destroyed using a P-4 rated shredder (or higher rating) when the defined business need has expired.

12. PATCH MANAGEMENT

Only licensed copies of commercial software which comply with and do not compromise security standards shall be used. Supplier shall follow a patching process and/or schedule for all infrastructure, systems and application products used to provide Services that includes the deployment of updates or upgrades in accordance with industry best practice. When vulnerabilities are revealed and can be addressed by a vendor patch, Supplier shall obtain the patch from the applicable vendor and apply it without delay in accordance with Supplier's then current vulnerability management and security patch management standard operating procedure or policy and only after such patch is tested and determined to be safe for installation in Supplier systems. Supplier shall ensure that vulnerability patches, antivirus and malware protection software are applied and kept up to date and shall not knowingly or intentionally introduce any harmful code into Supplier or RWS systems.

13. SECURITY INCIDENT RESPONSE

To ensure the proper implementation of incident management measures, the Supplier shall implement the following:

- Supplier shall establish procedures for identifying and reporting security incidents. This shall include the use of security monitoring tools, security awareness training for employees, and clear communication channels for reporting incidents;
- Supplier shall establish a process for categorizing and prioritizing security incidents based on severity and potential impact on the confidentiality, integrity, and availability of the data and information;

- Supplier shall establish procedures for responding to security incidents in a timely and effective manner. This will include the use of incident response teams, escalation procedures, and documented response plans for different types of incidents;
- Supplier shall conduct a thorough analysis and investigation of security incidents to determine the root cause and prevent similar incidents from occurring in the future;
- Supplier shall maintain accurate and detailed records of all security incidents, including the actions taken to resolve them. These records can be used for reporting, analysis, and compliance purposes.

Supplier shall notify RWS promptly (and in any event within 24 hours of becoming aware) of an actual or suspected security incident including a Personal Data Incident by emailing supplierincident@rws.com. Security incidents include but are not limited to extortion threats, unauthorized access, compromised user accounts or systems used to access, process or store Personal Data, the loss of any hard copy, hardware or storage media used to store or process Personal Data, or the infection of any system with malware such as computer viruses or ransomware.

14. ENDPOINT SECURITY

Personal Data shall only be stored on Supplier owned equipment and assets as required to fulfil a business need. The Supplier shall at a minimum implement appropriate measures to secure their endpoints (such as laptops, desktops, and mobile devices) and prevent unauthorized access to Personal Data and information provided by RWS, including:

- Install anti-malware software on all devices to detect and remove malware and viruses, and keep virus definitions up to date;
- Implement an automatic session lockout after a pre-defined period of inactivity;
- Enable host-based firewall protection on all endpoint devices are enabled;
- Regularly update all endpoint devices with the latest security patches and software updates to protect against known vulnerabilities;
- Install hard drive encryption on all endpoint devices to protect data in case of theft or loss of the device;
- Implement access controls on endpoint devices to ensure only authorized personnel can access the device and Personal Data stored on it;
- Implement regular backups and data synchronization;
- Implement a mobile device management system for mobile devices to ensure secure access and control over any Personal Data stored or accessed from these devices;
- Provide regular training to employees on best practices for endpoint security, including complying with the Supplier's security policy, how to avoid phishing attempts, how to recognize malware, and how to report suspected security incidents.

15. REMOVABLE MEDIA

Supplier shall not use removable media (USB, external hard drives, flash drives, CDs, DVDs, tapes, and other portable storage devices) to store Personal Data under any circumstances.

In any event, Supplier shall ensure Personal Data are adequately protected from unauthorized access, loss, and destruction in adherence with the terms outlined in this agreement and using industry-recognized controls.

16. NETWORK SECURITY

Supplier shall limit network flows to what is strictly necessary and implement secure remote access through VPN and secure its wireless Networks (WiFi) networks including by implementing the WPA3 protocol, wireless Networks (WiFi) shall use secure identification, authentication and encryption mechanisms; have "peer" networking connectivity settings disabled; prohibit insecure public WiFi use.

Supplier shall implement industry standard network access control measures to prevent unauthorized access to the data and information provided by RWS over the network. This can include the use of firewalls, intrusion detection and prevention systems, and other network security measures.

Supplier shall regularly monitor and test network security controls to ensure that they are functioning as intended.

17. BUSINESS CONTINUITY AND DISASTER RECOVERY

Supplier shall maintain a business continuity policy, strategy and program aligned to ISO 22301. Such a program shall maintain a business continuity plan which covers the services provided to RWS, the business continuity plan should be tested and reviewed periodically.

Supplier shall perform regular backups, encrypt and store backup media in a safe place, protect backups, especially during transport and regularly plan and test business continuity to ensure Personal Data can be restored in the event that the primary storage is unavailable.If Supplier is utilizing a datacenter to support services, Supplier shall have both a primary and backup datacenter in place, such datacenter can be maintained by Supplier or a third party.

18. ARCHIVING AND DISPOSAL

Supplier shall implement specific access rights to archived data and destroy expired archives securely.

When Supplier equipment, physical documents and files, and physical media are disposed of or reused, appropriate measures shall be taken to prevent subsequent retrieval of Personal Data originally stored in them. This may include restoring the device to its original configuration, degaussing or re-formatting of the storage media.

19. SUB-PROCESSORS AND THIRD-PARTY PROVIDERS

The Supplier shall implement appropriate measures to prevent unauthorized access to the data and information provided by RWS by sub-Suppliers and third-party providers (Third Parties), including:

- Ensure that Third Parties are selected based on their ability to comply with the security requirements for processing Personal Data;
- Regularly monitor and audit Third Parties to ensure that they are complying with the security requirements for the processing of Personal Data;

- Implement appropriate data flow controls to ensure that Personal Data is only shared with Third Parties that have been vetted and approved by the Supplier;
- Require Third Parties to report any security incidents or breaches involving Personal Data to the Supplier in a timely manner;
- Establish termination rights in the contracts with Third Parties in the event of non-compliance with the security requirements for processing Personal Data;
- Include specific data privacy and security clauses in Third Party contracts, stipulate the conditions for the return and destruction of data and ensure the effectiveness of the guarantees provided (e.g., security audits, visits).

20. SECURE SOFTWARE DEVELOPMENT

As applicable, Supplier shalldevelop secure applications for RWS and maintain a secure software development lifecycle which meets ISO 27001 standards.

Applications and websites developed and/or maintained by the Supplier shall have verification to ensure no passwords or Personal Data pass through URLs. Supplier shall regularly check that user input matches what is expected and implement a consent banner for cookies including a cookie policy for the service provided.

Supplier shall ensure logical separation between development environments and that of production and shall never use production or 'live' data from RWS for development and testing.

Supplier shall not promote software to production without addressing discovered vulnerabilities.

21. SECURITY TESTING

The Supplier shall implement appropriate measures to discover and address vulnerabilities in the Suppliers' systems, applications and network, including but not limited:

- Conduct regular vulnerability scanning of the Suppliers' systems, applications and networks to identify potential security vulnerabilities, testing should be performed for OWASP Top 10+ vulnerabilities using industry recognized tools.
- Establish a patch management process to ensure that security patches and updates are promptly applied to address known vulnerabilities, for critical or high-risk vulnerabilities, this should not exceed more than 30 days from the point of discovery;
- Conduct regular risk assessments to identify potential vulnerabilities and prioritize their remediation based on the level of risk they pose to Personal Data;
- Conduct regular testing of the Suppliers' systems and networks to ensure that security controls are effective and to identify any new vulnerabilities;
- Ensure that third-parties used by the Supplier for services such as cloud computing or network monitoring also address vulnerabilities in their systems and networks; Supplier shall contract with independent third-parties to perform penetration tests on its solutions to identify risks and remediation that help increase security during the Term of the Main Agreement and shall provide RWS third party penetration testing reports upon request.

22. INDEPENDENT VALIDATION OF CONTROLS

The Supplier commits to provide ISO 27001certification, and for providers of Infrastructure as a Service (IaaS), Software as a Service (SaaS) or otherwise any cloud services, SOC 2 type II attestation at time of contract signature and make them available to RWS for review.

Such attestation and certification shall be maintained throughout the term of the contract

The Supplier shall respond promptly to RWS reasonable enquiries from time to time for information about, or copies of, certifications and attestations mentioned above (and any updates or successors to them).

EXHIBIT 3 – DESCRIPTION OF THE PERSONAL DATA INCIDENT

Supplier shall notify RWS promptly (and in any event within 24 hours of becoming aware) of an actual or suspected Personal Data Incident by emailing supplierincident@rws.com with the completed form below:

Initial Report: Yes/No		**Follow-up Report:** Yes/No	
Contact Details of person reporting incident			
Potentially impacted RWS Personal Data			
Description			
What has happened?			
How did you find out about the incident?			
Which external third party was involved, if any?			
Has evidence of the incident been preserved?			
Timing and Geographical Location			
When did the incident start?		**Time (include time zone)**	
Is the incident ongoing?	**Yes/No**		
In which geographical location(s) has the incident occurred? Delete country that does not apply.	• Canada • North America • South America • UK • EU • Israel • Middle East, North Africa and Turkey	• South Africa • APAC • Australia • New-Zealand • China • Other:	
Nature of the Incident			
Is the incident a cyber incident?			
Has the incident potentially impacted the confidentiality, integrity and/or availability of RWS Personal Data? Indicate which.			

Personal Data and Individuals	
Which categories of RWS Personal Data are included in the incident?	
Indicate the approximate volume of RWS Personal Data.	
Which categories of individuals are potentially impacted?	
Indicate the approximate number of individuals.	
Mitigation	
Describe the actions taken to mitigate any potentially adverse effect.	
Describe the measures put in place or planned to eradicate the incident.	
Describe the measures put in place or planned to avoid incident from being repeated.	
Notifications	
Whom have you notified internally (and/or should the case arise, externally)?	

EXHIBIT 4 - LIST OF AUTHORISED SUB-CONTRACTORS

...

Legal name under which Supplier Subcontractors are registered	Address of establishment of Supplier Subcontractors	Description of Personal Data Processing by Supplier Sub-Contractors

Authorised Subcontractors will be specified in the relevant Order Form.