DATA PROCESSING AGREEMENT

This Data Processing Agreement and all of its Appendices (“DPA”) sets forth obligations of RWS, on behalf of itself and Affiliates (collectively “RWS”) and Client in relation to personal data processing activities performed by RWS on behalf of Client under the agreements pursuant to which RWS provides services to Client (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. **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;

1.2. **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;

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

1.4. **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;

1.5. **Data Subject** means the individuals whose personal data is processed by RWS under this DPA;

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

1.7. **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;

1.8. **Instructions** means Client documented instructions to RWS, 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 Client to RWS during the term of the Main Agreement and relating to the processing of personal data;

1.9. **Personal Data** means any information relating to an identified or identifiable natural person defined under the Data Protection Laws and that RWS processes on behalf of Client and under its Instructions as Data Processor or subprocessor;

1.10. **Personal Data Incident(s)** means an actual breach of security relating to Personal Data in RWS’s systems, facilities or equipment and/or RWS’s subcontractors’ 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;

1.11. **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 Personal Data;

1.12. **Security Policy** means the minimum-security requirements to be applied by RWS when Processing Personal Data to fulfil the services described under the Main Agreement;

1.13. **Sub-Processor** means any third party or where applicable a RWS 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);

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

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

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

2. GENERAL PROCESSING TERMS

2.1 Purpose Limitation

2.1.1 The Parties agree that RWS is providing Services as defined in the Main Agreement, acting as Processor or Sub-Processor as the case may be, to Client, acting accordingly as Data Controller or Data Processor.

2.1.2 RWS shall carry out the Processing of Personal Data under Client 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 RWS is subject; in such a case, RWS shall inform Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.1.3 Client shall have sole and full responsibility for the accuracy, quality and legitimacy of the Personal Data and the appropriate legal bases relied upon by Client and comply with all applicable Data Protection Laws in connection with this DPA. Client is solely and fully responsible for obtaining all necessary consents for the collection and Processing of any Personal Data. Where applicable, Client shall inform RWS without undue delay of any Data Subject consent withdrawal that would require RWS to proceed with a data deletion.

2.1.4 RWS shall inform Client if, in its opinion, an Instruction infringes Data Protection Laws.

2.1.5 The subject matter and description of the Processing of Personal Data by RWS is detailed under the Main Agreement.

2.2 Confidentiality

RWS shall ensure that all personnel of RWS and RWS 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. RWS 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 RWS shall ensure that all Authorized Personnel have received appropriate privacy and security training.

2.3 DPIA

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

3. ASSISTANCE AND COOPERATION

3.1 At Client request, RWS shall provide without delay all necessary assistance to fulfil Client obligation to respond to any request or inquiry Client 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.

3.2 RWS shall also without delay inform the Client 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.

3.3 RWS 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 Client unless notification to Client is prohibited by applicable law.

4. DATA SECURITY

4.1 Security Measures

4.1.1 RWS shall take appropriate administrative, technical and organizational measures as described under Exhibit B, to ensure the confidentiality, integrity, availability and resilience of RWS systems, Processes and procedures that involve the Processing of Personal Data.

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

4.1.3 Throughout the term of the Agreement, RWS will maintain a written 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 unauthorized Processing of, Personal Data.

4.1.4 At a minimum, RWS agrees to maintain a recognized standard of security either certified to ISO27001 or SOC2, the scope of which contains the Security Measures identified at Exhibit B. 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 newly 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.

4.2 Personal Data Incident

4.2.1 RWS 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, RWS shall:

a. notify Client of the Personal Data Incident by submitting written information via email to Client without undue delay, and in any event within 72 hours, such notification to include a description of the Personal Data Incident;

b. take immediate steps to contain the Personal Data Incident and mitigate its consequences;

c. investigate the Personal Data Incident.

d. collaborate with Client to determine the appropriate responses and mitigation actions as necessary or required under applicable law.

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

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

5. LIMITATION OF LIABILITY

5.1 Either party shall be liable to the other for all direct losses and damages incurred because of a material breach of this DPA and/or Data Protection Laws, or as a result of a Personal Data Incident.

5.2 Notwithstanding anything stated elsewhere in this DPA, liability under this DPA shall be subject to exclusions and limitations of liability provisions in the Main Agreement.

5.3 For the avoidance of doubt, the Client acknowledges and agrees that the total liability of RWS and its Affiliates for all claims from Client or its Affiliates arising out of or related to the Main Agreement and this DPA shall apply in aggregate for all claims under both the Main Agreement and this DPA.

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.

6.2 **EU SCCs**

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

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

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

iii. Module 3 (Processor to sub-Processor) will apply when RWS Processes the Personal Data as a Data Processor on behalf of third party as a Data Controller. Then the Client acting as a Data Exporter will transfer the Personal Data to RWS. RWS 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 2 "General 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 A and Exhibit B to this DPA;

x. Annex III of the EU SCCs shall be deemed completed with the information set out in Exhibit C 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 complete as follows:

i. Table 1 shall be deemed completed with the information set out in Exhibit A of the 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 A and Exhibit B of this DPA 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.

6.4 EU-US Data Privacy Framework

6.4.1 RWS Affiliates based in the US are registered under the EU-US Data Privacy Framework and/or Swiss-US Data Privacy Framework. The processing by RWS and RWS Affiliates in the US will be under the Data Privacy Framework in accordance with the Data Privacy Framework Principles in addition to obligations under the EU SCCs and/or UK Addendum.

6.4.2 RWS have certified to the US Department of Commerce that they adhere to the EU-US Data Privacy Framework Principles (EU-US DPF Principles) regarding the processing of personal data received from the European Union (EU) and the UK in reliance on the EU-US DPF and the UK Extension to the EU-US DPF.

6.4.3 RWS have also certified to the US Department of Commerce that they adhere to the Swiss-US Data Privacy Framework Principles (Swiss-US DPF Principles) regarding the processing of personal data received from Switzerland in reliance on the Swiss-US DPF.

7. SUB-PROCESSORS

7.1 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. Linguistic contractors and subject-matter experts;

ii. Data Centre hosting providers

7.2 Client grants RWS general written authorization to engage with (i) the categories of Sub-Processors in section 7.1 and as per Exhibit C; and (ii) new categories of Sub-Processors provided that RWS gives Client reasonable prior notice, together with relevant information. Client may object to the appointment of any new category of Sub-Processor within ten (10) days of receipt of the aforementioned notice, in written form upon data protection grounds. RWS will provide a detailed list of Sub-Processors to Client upon request.

7.3 If Client does not object to the engagement of a third party in accordance with Section 7.2 within ten (10) days of notice by RWS, that third party will be deemed an authorized Sub-Processor for the purposes of this DPA.

7.4 Any Sub-Processor engaged by RWS shall be contractually bound by way of a written contract that provides for data confidentiality, privacy and security obligations equivalent to those binding RWS under the Main Agreement and this DPA.

7.5 If a RWS Sub-Processor Processes Personal Data in a Third Country, RWS 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.

7.6 In any event, RWS shall remain liable for all acts and omissions of its Sub-Processors with respect to the Personal Data processed.

8. DELETION OF PERSONAL DATA

Upon termination of this DPA or the Main Agreement or after the end of provision of Services, RWS will delete Personal Data and all copies thereof or return to Client all documented physical Personal Data in its possession or control, unless otherwise agreed by Client and RWS.

9. AUDITS

9.1 The client shall have upon prior written notice of forty five (45) days the right to carry out no more than once in any 12 (twelve) consecutive months an audit of RWS information necessary to demonstrate compliance with this DPA and its Appendices. RWS shall provide Client all necessary assistance. Each party will pay for its own related costs. 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).

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

9.3 **Audit Findings**

Where an audit, whether performed by RWS or Client, reveals a data security risk and/or privacy compliance risk that may impact on the protection of Personal Data, or reveals a Personal Data Incident, breach or non-compliance of this DPA and/or Data Protection Laws, RWS shall without undue delay develop mitigation or rectification steps as applicable.

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 10.

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 A – DESCRIPTION OF THE PERSONAL DATA PROCESSING / TRANSFER

Data exporter: Client

Name, address and contact details: Provided in the DPA.

Activities relevant to the data transferred under these Clauses: Provided in the DPA.

Signature and date: Provided in the DPA.

Data exporter's role: ☐ Client is Data Controller/ ☐ Client is Data Processor

Data importer: RWS

Name, address and contact details: Provided in the DPA.

Activities relevant to the data transferred under these Clauses: Provided in the DPA.

Signature and date: Provided in the DPA.

Data importer's role: ☐ RWS is a Data Processor/ ☐ RWS 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.

Category	**Description**	
Categories of data subjects whose personal data is transferred	Client employees	☐
	Client's contractors, consultants, freelancers, contingent workers and/or temporary agency workers	☐
	Client's job applicants/candidates	☐
	Client End customers	☐
	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 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.	All categories below	□
	None of the categories below	□
	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 Client's (as data exporter) instructions in connection with the Services provided by RWS (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 Client to enable:	
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Necessary for the provision of Services	
For transfers to (sub-) processors, also specify subject	Describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the	

matter, nature and duration of the processing	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 substantially same as the security requirements set out in the Exhibit 2 of the DPA between the Data Exporter and Data Importer.

EXHIBIT B – SECURITY POLICY

This Security Policy outlines the minimum security and data privacy obligations that RWS shall meet when processing Client Content, which may include Personal Data (together, "Client Content"), in connection with the provision of Services under the Main Agreement. These obligations are in addition to, and do not limit, any other obligations set forth in the Agreement.

All capitalised terms not defined in this Security Policy shall have the meanings ascribed to them in the Main Agreement or the applicable Data Processing Agreement ("DPA").

1. LIABILITY

RWS expressly accepts responsibility for ensuring that the obligations set out in this Security Policy are fulfilled when processing Client Content, whether directly or indirectly through its Sub-Processors and/or third-party contractors (collectively referred to as "RWS" for the purposes of this Policy).

2. BINDING POLICIES AND PROCEDURES

2.1. RWS shall maintain documented and binding security and privacy policies and procedures ("Security Documentation") that comply with applicable Data Protection Laws and incorporate the requirements set out in this Security Policy. RWS shall ensure that such documentation is regularly reviewed and kept up to date.

2.2. The Security Documentation shall clearly define the physical, technical, and organisational measures implemented by RWS to protect Client Content against unauthorised access, acquisition, use, disclosure, or destruction. Upon request, RWS shall provide the Client with evidence that the Security Documentation is in place and current.

3. INFORMATION SECURITY PROGRAM

RWS shall implement and maintain an information security program, supported by a suite of policies and an organisational structure aligned with industry best practices. The program shall define clear roles and responsibilities and include the appointment of a senior management representative responsible for overseeing its implementation and ongoing maintenance. The representative shall have the authority to allocate resources and make decisions necessary to ensure the security of Client Content processed under the Main Agreement and shall report directly to RWS senior management. RWS shall regularly review and update the information security program to address emerging threats, vulnerabilities, and applicable regulatory requirements.

4. RISK MANAGEMENT

RWS shall conduct periodic, independent security risk assessments to identify the criticality of information assets, assess threats, evaluate potential risks, and implement appropriate risk treatment plans. RWS shall apply technical and organisational measures to mitigate identified risks, ensuring a level of security appropriate to the nature and severity of the risk.

5. INVENTORY

RWS shall maintain an inventory of media, servers, and equipment containing Client Content to ensure traceability and accountability. This inventory shall include records of the return or secure destruction of Client Content in accordance with applicable data retention and disposal policies.

6. PERSONNEL

RWS shall require all personnel to sign a non-disclosure or confidentiality agreement that outlines their responsibilities for protecting Client Content and the consequences of non-compliance. RWS shall provide annual training and awareness programs on information security and data protection to all personnel, ensuring they understand their obligations and are equipped to handle Client Content securely.

7. USER AUTHENTICATION

Access to RWS systems shall be strictly conditional upon the proper implementation and adherence to authentication procedures, in accordance with an approved Identity and Access Management (IAM) policy. Each user shall be assigned a unique login account, and authentication shall be enforced through secure mechanisms to prevent unauthorised access.

8. ACCESS MANAGEMENT

RWS shall enforce password policies that comply with applicable regulatory requirements, industry standards, and recognised best practices. Passwords shall be changed at least every 180 days, must not be reused, disclosed to others, or written down. Users shall be required to change any password assigned automatically or by an administrator. Systems shall enforce account lockout mechanisms to limit the number of failed login attempts and prevent unauthorised access.

9. ACCESS PRIVILEGES

Access privileges shall be granted based on predefined roles aligned with job responsibilities and the principle of least privilege. RWS shall ensure that access to Client Content is restricted on a need-to-know basis. Outdated or unnecessary access rights shall be promptly revoked, and access permissions shall be reviewed at least annually. RWS shall implement separation of duties controls to ensure that personnel with privileged access do not simultaneously have access to other sensitive systems or data beyond their role requirements.

10. ENCRYPTION, HASHING AND SIGNING

10.1. RWS shall use recognised, secure cryptographic algorithms, libraries, and software to protect Client Content. All secrets and cryptographic keys shall be securely stored and managed in accordance with industry best practices.

10.2. Client Content shall be protected equally, regardless of classification, both in transit outside of RWS's network and at rest. This includes, but is not limited to:

- Use of strong encryption algorithms, such as Advanced Encryption Standard (AES), to prevent unauthorised access;
- Secure generation, storage, rotation, and destruction of encryption keys, ensuring sufficient key length and randomness to prevent brute-force attacks;
- Secure transmission of Client Content using protocols such as Transport Layer Security (TLS);
- Encryption of Client Content at rest using secure algorithms and key management practices;
- Compliance of encryption methodologies with applicable laws and regulations;
- Encryption of Client Content prior to transmission to authorised external parties, with secrets (e.g., decryption keys) transmitted separately via a different communication channel to ensure confidentiality.

11. LOGGING

RWS shall maintain appropriate audit trails and system access logs for all Information Systems processing Client Content. Logs shall be protected against tampering and monitored by trained security personnel to detect anomalies and support incident investigation and compliance requirements.

12. PHYSICAL AND ENVIRONMENTAL SECURITY

RWS shall implement physical and environmental security measures to prevent unauthorised physical access, damage, or interference to Client Content and supporting infrastructure. These measures shall include, but are not limited to:

- Physical access controls to restrict access to authorised personnel only, including mechanisms such as locked doors, access cards, biometric systems, and security guards;
- Environmental controls to mitigate risks from fire, flooding, temperature fluctuations, and power outages, including fire suppression systems, water detection, HVAC systems, and backup power supplies;
- Asset management controls to track and manage equipment, hardware, and software that store or process Client Content, including inventory systems, asset tagging, and regular inspections;
- Secure work areas with restricted access, surveillance, and physical safeguards to prevent unauthorised access or theft;
- Documented physical security policies and procedures aligned with industry standards, covering access control, environmental protection, asset management, and incident response;
- Monitoring and testing of physical security controls through regular inspections and audits;
- Secure destruction of sensitive materials, including the use of P-4 rated shredders (or higher) for hard copy records, and physical destruction of decommissioned hard drives and storage media;
- Physical access restrictions and monitoring at data centre facilities, which may include multi-zone security, mantraps, perimeter deterrents (e.g., fencing, guarded gates), biometric access, CCTV, and secure cages;
- Protection of equipment and media used to process Client Content from physical and environmental threats, including secure storage when not in use;
- Secure storage of hard copy records containing Client Content in filing systems that support retrieval, amendment, and destruction in accordance with data subject rights;
- Use of locked containers or equivalent secure transport mechanisms for moving hard copy records, and secure destruction of such records when no longer required.

13. PATCH MANAGEMENT

13.1. RWS shall ensure that only licensed software is used in the provision of services and that such software complies with applicable security standards. RWS shall maintain a documented patch management process and schedule covering all infrastructure, systems, and application components used to deliver services. This process shall include the timely deployment of updates and upgrades in accordance with industry best practices.

13.2. When a vulnerability is identified and a vendor patch is available, RWS shall obtain the patch from the relevant vendor and apply it in accordance with its current vulnerability and security patch management policies and procedures. Patches shall only be deployed after appropriate testing to confirm their stability and compatibility with RWS systems. RWS shall ensure that vulnerability patches, antivirus, and anti-malware protections are applied and kept up to date, and shall not knowingly or intentionally introduce any malicious code into RWS or Client systems.

14. SECURITY INCIDENT RESPONSE

RWS shall implement and maintain an incident response framework to ensure the timely identification, management, and resolution of security incidents. This shall include:

- Procedures for identifying and reporting security incidents, supported by security monitoring tools, employee awareness training, and clearly defined communication channels;
- A process for categorising and prioritising incidents based on severity and potential impact on the confidentiality, integrity, and availability of data and systems;
- Documented response procedures, including escalation paths and the involvement of incident response teams, tailored to different types of incidents;
- Root cause analysis and post-incident reviews to prevent recurrence of similar incidents;
- Maintenance of accurate and detailed records of all security incidents, including actions taken, for audit, compliance, and reporting purposes.

RWS shall notify the Client without undue delay, and in any event within 72 hours of becoming aware of a security incident that impacts the Client, including any Personal Data Incident. Notification shall be sent to the Client's designated contact email address.

15. ENDPOINT SECURITY

Client Content shall only be stored on RWS-owned equipment and assets where necessary to fulfil a defined business purpose. RWS shall implement appropriate endpoint security measures to protect against unauthorised access to Client Content and other sensitive information. These measures shall include, at a minimum:

- Installation and maintenance of anti-malware software on all endpoint devices, with up-to-date virus definitions;
- Automatic session lockout after a predefined period of inactivity;
- Activation of host-based firewall protection on all endpoint devices;
- Regular application of security patches and software updates to protect against known vulnerabilities;
- Full-disk encryption on all endpoint devices to protect data in the event of loss or theft;
- Access controls to ensure only authorised personnel can access endpoint devices and any Client Content stored on them;
- Regular backups and data synchronisation to ensure data availability and integrity;
- Ongoing employee training on endpoint security best practices, including adherence to RWS's security policies, phishing awareness, malware identification, and incident reporting procedures.

16. REMOVABLE MEDIA

16.1. RWS shall not use removable media (including USB drives, external hard drives, flash drives, CDs, DVDs, tapes, or other portable storage devices) to store Client Content under any circumstances.

16.2. Regardless of media type, RWS shall ensure that Client Content is protected against unauthorised access, loss, or destruction using industry-recognised security controls and in accordance with the terms of this agreement.

17. NETWORK SECURITY

17.1. RWS shall implement appropriate network security controls to ensure the confidentiality, integrity, and availability of systems and data. Network flows shall be restricted to what is strictly necessary, and secure remote access shall be enforced through the use of Virtual Private Networks (VPNs). Wireless networks (Wi-Fi) shall be secured using WPA3 or equivalent encryption protocols, and shall include secure identification, authentication, and encryption mechanisms. Peer-to-peer networking shall be disabled, and the use of insecure public Wi-Fi shall be prohibited.

17.2. RWS shall implement industry-standard network access controls to prevent unauthorised access to systems and data. These controls may include firewalls, intrusion detection and prevention systems (IDPS), extended detection and response (XDR), and other appropriate technologies. RWS shall regularly monitor and test network security controls to ensure they are functioning effectively.

18. BUSINESS CONTINUITY AND DISASTER RECOVERY

18.1. RWS shall maintain a business continuity management system aligned with ISO 22301, including a documented business continuity policy, strategy, and program. This program shall include a business continuity plan covering the services provided by RWS, which shall be reviewed and tested periodically to ensure effectiveness.

18.2. RWS shall perform regular backups of critical systems and data, ensure that backup media is encrypted and securely stored, and implement appropriate protections during transport. Business continuity and disaster recovery procedures shall be tested regularly to ensure that Client Content can be restored in the event of a disruption. Where RWS utilises data centres to support its services, both primary and backup data centres shall be in place. These data centres may be operated by RWS or by approved third-party providers.

19. DISPOSAL

19.1. In the event that client data is archived, RWS shall implement appropriate access controls for archived data to ensure that only authorised personnel can access such data. Expired archives shall be securely destroyed in accordance with RWS's data retention and disposal policies.

19.2. When disposing of or repurposing equipment, physical documents, files, or media containing Client Content, RWS shall implement appropriate measures to prevent unauthorised recovery of the data. Such measures may include secure deletion, reformatting, degaussing, or restoring devices to their original configuration.

20. SUB-PROCESSORS AND THIRD-PARTY PROVIDERS

RWS shall implement appropriate controls to prevent unauthorised access to Client Content by sub-processors and third-party providers ("Third Parties"). These controls shall include:

- Conducting security risk assessments of Third Parties and approving their use based on their ability to meet RWS's security requirements for processing Client Content;
- Regularly monitoring Third Parties to ensure ongoing compliance with applicable security requirements;
- Implementing data flow controls to ensure Client Content is only shared with vetted and approved Third Parties;
- Requiring Third Parties to report any security incidents or data breaches involving Client Content to RWS in a timely manner;
- Including termination rights in contracts with Third Parties in the event of non-compliance with security obligations;

- Incorporating specific data privacy and security clauses in Third Party contracts, including provisions for the return or secure destruction of Client Content.

21. SECURE SOFTWARE DEVELOPMENT

21.1. Where applicable, RWS shall develop secure applications for the Client and maintain a secure software development lifecycle (SDLC) aligned with ISO/IEC 27001 standards. Applications and websites developed and/or maintained by RWS shall be designed and tested to ensure that passwords and Personal Data are not transmitted via URL query strings or other insecure mechanisms.

21.2. RWS shall implement input validation controls to ensure that user input conforms to expected formats and does not introduce security vulnerabilities.

21.3. RWS shall ensure logical separation between development and production environments.

21.4. RWS shall not promote software to production without first addressing all discovered vulnerabilities classified as critical or high risk, in accordance with industry-standard vulnerability scoring systems (e.g., CVSS).

22. SECURITY TESTING

RWS shall implement appropriate measures to discover and address vulnerabilities in RWS systems, applications and network, including but not limited:

- Conduct regular vulnerability scanning of RWSs' 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;
- Conduct risk assessments to identify potential vulnerabilities and prioritize their remediation based on the level of risk they pose to Client Content; If applicable, ensure that Third Parties used by RWS for services such as cloud computing or network monitoring also address vulnerabilities in their systems and networks.
- RWS shall engage independent Third Parties to conduct penetration testing on its web applications to identify security vulnerabilities. These tests will be performed at a minimum prior to each major release of the web application. RWS shall mitigate identified vulnerabilities according to defined security policy expectations and, upon request, provide the Client with executive summary reports of the third-party penetration testing.

23. INDEPENDENT VALIDATION OF CONTROLS

23.1. RWS commits to maintaining an independent security certification, such as ISO/IEC 27001 or SOC 2 Type II, at the time of contract signature. These certifications shall be made available to the Client for review upon request. Such certifications or attestations shall be maintained throughout the term of the contract.

23.2. RWS shall respond promptly to reasonable requests from the Client for information about, or copies of, these certifications and attestations, including any updates or successor certifications that may apply.

EXHIBIT C - LIST OF AUTHORISED SUB-PROCESSORS

...

Legal name under which RWS Sub-Processors are registered	Address of establishment of RWS Sub-Processors	Description of Personal Data Processing by RWS Sub-Processors
• Linguistic contractors and subject-matter experts • Data center hosting providers		

Authorised Sub-Processors may be further specified in the relevant Order Form.