DATA PROTECTION ("DP") ANNEX
(Processor to Controller)

1. INTRODUCTION

1.1 This DP Annex is entered into

(1) "Hottinger Bruel & Kjaer UK Limited" (the **Supplier**)	(2) Entity that accesses and/or uses the Reliasoft Cloud software under the End User License Agreement and the Software as a Service (SaaS) Service Agreement (the **Customer**)

1.2 each a **Party** and together the **Parties.**

2. GENERAL

2.1 This DP Annex is an annex to the Agreement and sets out the additional terms, requirements and conditions to which Customer will Disclose and the Supplier will Process Personal Data in relation to the services to be performed under the Agreement. This DP Annex contains mandatory clauses required by Applicable Data Protection Law(s) for contracts between controller and processors.

2.2 Terms used in the DP Annex have the same meaning as those used in the Agreement, unless explicitly provided otherwise in Clause 16. In this DP Annex, unless the contrary intention appears, a reference to a clause, schedule or appendix is a reference to a clause, schedule or appendix of or to this DP Annex. The appendixes form part of this DP Annex.

2.3 If there is any conflict or inconsistency between a term in the body of this DP Annex and a term in the Agreement, or in any of the schedules or other documents referred to or otherwise incorporated into this DP Annex, the following hierarchy of precedence shall apply:

(a) the provisions of any Model Contract;

(b) a term in the body of this DP Annex;

(c) a term in an appendix of this DP Annex; and

(d) the provisions of the Agreement.

2.4 The DP Annex is agreed between Customer and Supplier, on Supplier's own behalf, and on behalf of and for the benefit of Supplier's Affiliates, on behalf of which Supplier is entitled to enforce any and all of the provisions of the DP Annex. For purposes of the DP Annex, "Supplier" also means each of its Affiliates, unless explicitly provided otherwise. Supplier's Affiliates are entitled to enforce the provisions of the DP Annex as though those Affiliates were the Supplier.

3. ROLES

3.1 Customer and Supplier acknowledge that that status of each party is a question of fact determined by the Applicable Data Protection Law(s).

3.2 Without limiting Clause 3.1, Customer and Supplier acknowledge that, it is their mutual understanding

(a) that in relation to the Processing of Personal Data in the context of the services under the Agreement, Customer is Controller and Supplier is Processor;

(b) subject to Clause 3.2(c), Supplier can appoint Sub-Processor(s) to Process Personal Data on its behalf; and

(c) if and to the extent that any Processing undertaken by Sub-Processor(s) involves an international transfer that Processing shall be undertaken by Sub-Processor(s) as Processor for an on behalf of Customer pursuant to the applicable Model Contract in accordance with clause 13.3.

4. INSTRUCTIONS

4.1 When carrying out the Processing services, Supplier shall act only on the instructions from Customer and for the purposes authorised by Customer, unless Supplier is otherwise required to Process Personal Data under the applicable laws to which it is subject.

4.2 The parties acknowledge that nothing in this DP Annex constitutes a transfer or assignment of any rights in Personal Data (including any intellectual property rights) unless otherwise expressly set out in the Agreement.

4.3 Customer hereby instructs Supplier to Process Personal Data in accordance with the specifications set out in Appendix 1 (Data Processing Specifications) to this DP Annex. The Agreement and the DP Annex are Customer's complete and final instructions to Supplier for the Processing, except to the extent agreed otherwise by the Parties.

5. APPLICABLE LAW

5.1 When carrying out the obligations under the Agreement Supplier shall use reasonable endeavours to comply with the Applicable Processor Law(s).

5.2 Customer shall in its Processing of Customer Data comply with, and be liable for non-compliance with, all Applicable Data Protection Law(s) and other applicable laws such as employment law, local laws on employee monitoring, works council approvals and criminal law.

5.3 Each Party shall deal with reasonable requests for assistance from the other Party to ensure that the Processing complies with Applicable Data Protection Law(s).

6. SECURITY

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Supplier shall implement appropriate technical, physical and organisational security measures appropriate to the risk, in particular to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised Disclosure or access, and against all other forms of unlawful Processing including, but not limited to, unnecessary collection or further Processing. The measures that Supplier shall take are specified in Appendix 2 (Security Measures) to the DP Annex, which Appendix Supplier shall revise if so required to reflect industry standards.

7. NON-DISCLOSURE AND CONFIDENTIALITY

7.1 Supplier shall keep Customer Data confidential and shall not Disclose Customer Data in any way to any Employee or Third Party without the prior written approval of Customer, except where (i) subject to Clause 7.2 of this DP Annex, the Disclosure is required for the performance of the Processing, or

(ii) subject to Clause 9.1(b) of this DP Annex, where Customer Data need to be Disclosed to a competent public authority to comply with a legal obligation or as required for audit purposes.

7.2 Supplier shall use reasonable endeavours to provide the Employees with access to Customer Data only to the extent necessary to perform the Processing. Supplier shall ensure that any Employee it authorises to have access to Customer Data Processed on behalf of Customer has been made aware of the confidentiality and security of the Customer Data.

8. SUB-PROCESSORS

Notwithstanding Clause 3.2(c) above, Customer hereby provides Supplier with a general written authorisation to engage Sub-Processors, provided that: (i) Supplier notifies Customer of the identity of the Sub-Processor thirty (30) days prior to the addition or replacement of a Sub-Processor; (ii) the Sub-Processor commits to act according to the instructions of Customer (which will be given through Supplier); (iii) Supplier shall ensure that Sub-Processors shall be contractually bound to protect Customer Data in terms that are no less protective than the terms of this DP Annex; and (iv) Supplier remains responsible for the Sub-Processors' compliance with this DP Annex.

9. NOTIFICATIONS OF DISCLOSURES AND PERSONAL DATA BREACHES

9.1 Supplier shall use reasonable efforts to inform Customer if:

(a) it receives an inquiry, a subpoena or a request for inspection or audit from a competent authority relating to the Processing, except where Supplier is otherwise prohibited by law from making such disclosure;

(b) it intends to Disclose Customer Data to any competent public authority; or

(c) it detects or reasonably suspects that a Personal Data Breach has occurred.

9.2 In the event of a Personal Data Breach, Supplier shall take reasonable remedial measures to preserve the confidentiality of the Customer Data. Furthermore, Supplier shall provide Customer with the information reasonably requested by Customer regarding the Personal Data Breach.

10. COMPLAINTS, REQUESTS AND ENQUIRIES

Supplier shall not independently respond to any complaints, requests or enquiries received from Individuals without Customer's prior written consent, except where required by law. Supplier will upon receipt, at its choice, either make reasonable efforts to refer the Individual to the Customer or make reasonable efforts to forward the Individual's complaint, request or enquiry to the Customer.

11. RETURN AND DESTRUCTION OF CUSTOMER DATA

11.1 All Customer Data shall be returned to Customer upon Customer's request. Supplier shall not retain Customer Data any longer than is necessary for the purposes of performing its obligations under the Agreement.

11.2 Upon termination of the Agreement, Supplier shall, at the option of Customer, return and/or delete the Customer Data and copies thereof to Customer and/or shall destroy such Customer Data, except to the extent the Agreement or applicable law provides otherwise. In that case, Supplier shall no longer Process the Customer Data, except to the extent required by the Agreement or applicable law.

12. SERVICE ANALYSIS

Supplier may compile statistical and other information related to the performance, operation and use of the services, and use data from the services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes**.**

13. TRANSFER

13.1 This Clause 13 applies only to international transfers of Personal Data by a Data Sender to a Data Recipient, including any onward international transfer.

13.2 Customer hereby authorises Supplier to enter into and execute on its behalf any UK Model Contract with any Third Party including Sub-Processor(s) or Supplier Affiliates to facilitate the international transfer of Personal Data where the Supplier acts as Data Sender for and on behalf of Customer.

13.3 The Data Sender shall only Process or transfer Personal Data in or, in the case of transfer, to, any country or territory outside the UK and EEA if and for so long as:

(a) an Adequacy Decision is in place;

(b) the international transfer or onward international transfer is subject to a derogation in accordance with Article 49 EU GDPR or Article 49 UK GDPR (as applicable);

(c) it is made in accordance with Article 46 EU GDPR or Article 46 UK GDPR (as applicable), including in accordance with the terms of Supplier's approved Processor Binding Corporate Rules or where a Model Contract is in place between the Data Sender and Data Recipient.

13.4 Appendix 4 (*Country Specific Addendum*) sets out local jurisdiction requirements relating to other international transfers other than from the EEA or the UK.

International transfer mechanism

13.5 If, in accordance with Clause 13.3(c) an international transfer or onward international transfer is required to be governed by a Model Contract, then:

(a) Subject to Appendix 3, the Data Sender and Data Recipient shall comply with the terms of that Model Contract;

(b) the relevant Data Sender shall assume all the rights, obligations and liability of the "data exporter" under the Model Contract; and

(c) the Data Recipient shall assume all the rights, obligations and liabilities of the "data importer" under the Model Contract.

13.6 If the mechanism for international transfers of Personal Data relied upon pursuant to Clause 13.3 ceases for any reason to be a valid means of complying with the restrictions on international data transfers as set out in Data Protection Laws, or otherwise ceases to apply for any reason, or the exporting Party determines that it does not provide appropriate protection for Personal Data in the circumstances, the parties shall act in good faith to agree the implementation of an alternative solution to enable both parties to comply with Data Protection Law(s).

14. LIMITATION ON LIABILITY

14.1 Any limitation of liability clause in the Agreement shall apply to this DP Annex.

15. NOTICES

15.1 All notices, confirmations and other statements made by the parties in connection with this DP Annex shall be in writing and shall be sent by email to:

Supplier: dataprotection@hbkworld.com

16. DEFINITIONS

In this DP Annex:

Adequacy Decision means, in respect of a third country, a territory, or one or more specified sectors within that third country, a finding of adequacy:

(a) pursuant to Article 45 of the EU GDPR; or

(b) pursuant to Article 45 of the UK GDPR,

in each case to the extent applicable to an international data transfer under this DP Annex;

Affiliate means in relation to either Party the ultimate parent company of that Party and any company, partnership or legal entity of which the ultimate parent company directly or indirectly owns more than 50% of the issued share capital or otherwise directs the activities of such other legal entity;

Agreement means Software as Service (SaaS) Service Level Agreement – Reliasoft Cloud

Applicable Data Protection Law(s) means the Data Protection Laws applicable to Customer or Supplier as Controllers;

Applicable Processor Law(s) means the Data Protection Laws that are applicable to Supplier as the Processor;

Controller means the entity or natural person which alone or jointly with others determines the purposes and means of the Processing;

Customer means Entity that accesses and/or uses the software under the End User License Agreement and the Software as a Service (SaaS) Service agreement;

Data Protection Law(s) means any law, enactment, regulation, or order concerning the processing of personal data relating to living persons including:

(a) UK Data Protection Laws, and

(b) EU Data Protection Laws

each to the extent applicable to the activities or obligations of the parties under or pursuant to this DP Annex;

Data Recipient means parties identified under Appendix 1 to this DP Annex which receive Personal Data from, or are given access to Personal Data by, the Data Sender under, or in connection with this DP Annex;

Data Sender means the parties identified in Appendix 1 to this DP Annex which transfer (via international transfer or otherwise) Personal Data to a Data Recipient or provides access to Personal Data to a Data Recipient under or in connection with this DP Annex;

Disclosure means any form of disclosure of Personal Data to (including remote access by) any Employee or any Third Party. **Disclose** and **Disclosed** are to be construed accordingly;

DP Annex means this data protection annex;

EC Standard Contractual Clauses means the EC Standard Contractual Clauses as published in the Decision of the European Commission of 4 June 2021 (Decision 2021/914);

EEA means all member states of the European Union, Iceland, Liechtenstein, Norway and, for the purposes of the DP Annex, Switzerland;

Employee means any employee, agent, contractor, work-for-hire or any other person working under the direct authority of Supplier;

EU Controller-Processor Model Contract means a data transfer agreement in the form adopted by EC Standard Contractual Clauses between a controller as "data exporter" and a processor as "data importer", as amended in accordance with Schedule (as amended, superseded or replaced from time to time);

EU Processor-Processor Model Contract means a data transfer agreement in the form adopted by EC Standard Contractual Clauses between a processor as "data exporter" and a processor as "data importer" (as amended, superseded or replaced from time to time);

EU Data Protection Law(s) means the EU GDPR, and any law, enactment, regulation or order transposing, implementing, adopting, supplementing or derogating from, the EU GDPR and the EU Directive 2002/58/EC in each Member State;

EU GDPR means EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

EU Model Contract means the EU Controller-Processor Model Contract or the EU Processor-Processor Model Contract;

Individual means any individual whose Personal Data is Processed by Supplier on behalf of Customer in the course of the performance of the Agreement;

Model Contract means an EU Model Contract or a UK Model Contract (as applicable);

Non-Adequate Country means a country that is deemed not to provide an adequate level of protection of Personal Data within the meaning of Article 45 of the EU GDPR or within the meaning of Article 45 of the UK GDPR;

Personal Data means any information relating to an identified or identifiable individual that is Processed by Supplier on behalf of Customer in the course of the performance of the Agreement;

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised Disclosure of, or access to the Personal Data of an Individual;

Processing means any operation that is performed on Personal Data, whether or not by automated means, such as collection, recording, storage, organisation, alteration, use, Disclosure (including the

granting of remote access), transmission or deletion of Personal Data. **Process** and **Processed** are to be construed accordingly;

Processor means the entity or natural person which Processes Personal Data on behalf of Controller;

Retained EU Law means retained EU Law as defined in the European Union (Withdrawal) Act 2018;

Sub-Processor means any Third Party, including Supplier's Affiliates, engaged by Supplier that Processes Personal Data under the instruction or supervision of Supplier; and

Supplier means "Hottinger Bruel & Kjaer UK Limited"

Third Party means any party other than the parties to the Agreement.

UK Data Protection Laws means the UK GDPR, the UK Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003;

UK GDPR means the General Data Protection Regulation 2016/679 as it forms part of Retained EU Law;

UK ICO means the United Kingdom Information Commissioner's Office;

UK Model Contract means either:

(a) **UK Processor-Processor Transfer Addendum**, a data transfer addendum to EU Processor-Processor Model Contract, in the form adopted by the UK ICO (as amended, superseded or replaced from time to time) as an international data transfer mechanism under UK GDPR; or

(b) **UK Controller-Processor Agreement**, consisting of either:

(i) **UK Controller-Processor Transfer Addendum**, a data transfer addendum to EU Controller-Processor Model Contract, in the form adopted by the UK ICO (as amended, superseded or replaced from time to time) as an international data transfer mechanism under UK GDPR, and as amended in accordance with; or

(ii) **UK Controller-Processor Model Contract**, a data transfer agreement in the form published by the UK Information Commissioner's Office at https://ico.org.uk/media/for-organisations/documents/2618973/uk-sccs-c-p-202012.docx and named "Standard contractual clauses for controllers to processors", between a controller as "data exporter" and a processor as "data importer", (as amended, superseded or replaced from time to time) and as amended in accordance with (if applicable).

In this DP Annex:

(a) any reference to a **transfer** means the sharing of, or the enabling of access to, personal data, by one party with another party, and "**transferred**" shall be construed accordingly;

(b) any reference to an **international transfer** (or equivalent) means a transfer of Personal Data by a party (as Data Sender) in one jurisdiction to another party (as Data Recipient) in another jurisdiction (excluding transfers between parties that are both within the EEA or the UK, whichever applies);

(c) any reference to an **onward international transfer** (or equivalent) means onward transfer of Personal Data, received by a Data Recipient pursuant to an international transfer, to a Data Recipient in another jurisdiction; and

(d) in this DP Annex any reference, express or implied, to an enactment (which includes any legislation in any jurisdiction) includes, except to the extent that the contrary intention appears: that enactment as amended, extended or applied by or under any other enactment (before, on or after execution of this DP Annex); any enactment which that enactment re-enacts (with or without modification); any subordinate legislation made (before, on or after execution of this DP Annex) under that enactment, including (where applicable) that enactment as amended, extended or applied, or under any enactment which it re-enacts.

APPENDIX 1

DATA PROCESSING SPECIFICATIONS

PROCESSING OF PERSONAL DATA BY SUPPLIER

Parties and roles	
Data Sender – entity sending the Personal Data	"Customer" acting as **Controller.**
Data Recipient – entity receiving the Personal Data	"Hottinger Bruel & Kjaer UK Limited" acting as **Processor.**
Description of processing	
Purposes	Personal information is used to authenticate and authorise the user and send notifications of support ticket. Support team might use contact information to reach out to customers.
Personal Data categories	*Include all that apply:* *- Name* *-Login ID.* *-Contact information (e-mail, phone numbers).* *-Log and Usage data* *Special category personal data* • None - the personal data being processed does not include any special categories of personal data.
Data subjects – the Personal Data Processed concern the following categories of individual	ReliaSoft Cloud Software User´s.
International Transfers	
Will the Processing of Personal Data involve any international transfers of Personal Data?	Yes
Frequency of international transfers of Personal Data	Continuous

Other items			
Duration of processing	The term of the Agreement		
Maximum retention periods	Upon termination of contract with a customer but no longer than 90 days after such termination, all personal data is removed from ReliaSoft Cloud. In relation to the personal data on the contract to perform the services it will be retained according to the legal retention periods.		
Sub-Processors	The Sub-Processor of the Data Recipient are indicated in the table below together with a description of the Processing activities they carry out.		
	Subject-matter of processing	***Nature of processing***	***Duration of processing***
Azure	Hosting of web application on K8s cluster	Azure hosts and manages the Kubernetes cluster, enabling containerized application deployment, scaling, and orchestration.	For the duration of the service agreement or until deletion.
	PostgreSQL database hosting and management	Azure provides storage, processing, and management of application data through a managed PostgreSQL database service.	For the duration of the service agreement or until deletion.
	Data analysis and processing	Azure utilizes Azure OpenAI to process data by deploying AI models that deliver AI-driven recommendations and insights.	For the duration of the service agreement or until deletion.
	Secrets management	Azure Key Vault securely stores and manages secrets, API keys, and credentials for application use.	For the duration of the service agreement or until deletion.
	User access and activity logs	Azure processes access credentials, usage logs, and activity data for auditing, monitoring.	Retained as per Azure's data retention policy or until account deletion.

Atlassian	Project and task management data	Atlassian processes project-related data, task assignments, comments, and file attachments for collaboration.	For the duration of the subscription or service agreement.
	Documentation and knowledge base management	Atlassian processes data to enable the documentation, sharing, and collaborative editing of policies, processes, agreements, and architectural documents.	For the duration of the subscription or service agreement.
	User access and activity data	Atlassian collects and processes user login credentials, usage logs, and user activity for authentication and auditing purposes.	Retained as per their data retention policy or until account deletion.
Github	Codebase storage and version control	GitHub stores and manages the codebase, including version history, branches, commits, and pull requests.	Data is retained as per GitHub's data retention policies or until the repository is deleted.
	Storage of assets (e.g., images, files)	GitHub stores associated assets such as images, documentation, or configuration files uploaded to the repositories.	Data is retained as per GitHub's data retention policies or until the repository is deleted.
	GitOps workflows	GitHub processes CI/CD pipeline configurations, deployment scripts, and automation workflows through GitHub Actions.	Data is retained as per GitHub's data retention policies or until the repository is deleted.
	User access and repository activity logs	GitHub processes user credentials, access logs, and activity history for	Data is retained as per GitHub's data retention

		collaboration, auditing, and security.	policy or until account deletion.
Grafana Labs	Storage and visualization of logs and metrics	Grafana processes and stores logs and metrics data for monitoring, analysis, and troubleshooting purposes.	Log, Traces and Profiles retention is 30 days. Metrics retention is 13 months
	Alerting and notifications	Grafana processes data to generate alerts based on predefined thresholds and sends notifications to users.	For the duration of the service agreement or until deletion. Alert History retention 7 days
	Incident management	Grafana processes incident-related data, such as logs, metrics, and user inputs, for root cause analysis and reporting.	For the duration of the service agreement or until deletion.
	User access and activity data	Grafana processes user credentials, access logs, and activity history for authentication and auditing purposes.	Retained as per Grafana's data retention policy or until account deletion.

APPENDIX 2

SECURITY MEASURES

1. Data in transit is protected by TLS encryption

2. Data protection from Unauthorised access:

   All access to ReliaSoft Cloud requires authentication. Authentication can be provided by ReliaSoft Cloud, or delegated to a customer's single-sign-on. Each customer is responsible for creating accounts for their users and assigning those users limited authorization within the ReliaSoft Cloud services. Every customer has fully segregated user data and authentication.

3. Data stored in Cloud is Secured by the following mechanism:

Compliance	HBK are in the process of aligning to ISO27001 and working towards compliance GDPR Compliance
Access	Only authorized users can access application data via a web browser ReliaSoft Cloud infrastructure fully fire-walled from the public Internet
Data Partitioning	ReliaSoft Cloud employs physical segregation of customer data, providing high-level confidentiality across tenants
Encryption	Encryption is employed for all data in-transit Encryption is employed for all data at-rest
Backup	Periodic rolling backups are performed for all persisted data Data can be recovered with minimal data loss
High Availability	Services are managed by cluster orchestration ensuring high availability Cluster orchestration redundantly deployed across multiple instances for zero downtime failover

APPENDIX 3

MODEL CONTRACTS

1. EU MODEL CONTRACT

1.1 To the extent a Data Sender and Data Recipient enter into EU Controller-Processor Model Clauses or the EU Processor-Processor Clauses, the EU Controller-Processor Model Clauses or EU Processor-Processor Model Clauses shall be amended as follows:

(a) **Clause 9 (Use of sub-processors):**

(i) "Option 2" applies unless agreed otherwise by the relevant parties; and

(ii) the Data Recipient must notify the Data Sender thirty (30) days prior to the addition of the replacement of the Sub-Processor;

(b) **Clause 13 (Supervision):**

(i) the member state of the relevant Data Sender (and the applicable Supervisory Authority); and

(ii) the member state where the relevant data subjects are located,

shall typically be determined by the "place of incorporation" of the relevant Data Sender set out in Appendix 1;

(c) **Clause 17 (Governing law):** The governing law shall be the laws of the Netherlands;

(d) **Clause 18 (Choice of forum and jurisdiction):** Disputes shall be resolved by the courts of the Netherlands;

(e) **Annex I.A** (List of parties):

(i) Appendix 1 of this DP Annex specifies:

(A) the Data Sender(s) acting as "data exporter(s)";

(B) the Data Recipient(s) acting as "data importers(s)"; and

(C) the purposes for which the Data Recipient may process Personal Data; and

(D) Appendix 1 sets out the contact details of each party's representative.

(f) **Annex I.B (Description of the transfer):** in respect of a transfer to a Processor, Appendix 1 of this DP Annex specifies:

(i) the categories of Data Subject whose Personal Data is transferred;

(ii) the Personal Data categories transferred (including special category data);

(iii) the purposes of the international transfer and further Processing;

(iv) if applicable, any additional safeguards that must be met in relation to the international transfer and Processing of special category Personal Data; and

(v) if applicable, the duration of processing and any maximum data retention periods;

(g) **Annex II (Technical and Organisational Measures):** Appendix 2 of this DP Annex sets out the technical and organisational measures that must be met by Data Recipients that are Processors; and

(h) **Annex III (List of Sub-Processors):** in respect of a transfer to a processor, Appendix 1 of this DP Annex specifies the permitted Sub-Processors.

2. UK MODEL CONTRACT

2.1 To the extent the Data Sender and Data Recipient enter into a UK Controller-Processor Transfer Addendum pursuant to Clause 13.3 of this DP Annex:

(a) the date of the UK Controller-Processor Transfer Addendum is the date of acceptance of the Software as a Service (SaaS) Service Level Agreement;

(b) the clauses of the EU Controller-Processor Model Contract are incorporated into the UK Controller-Processor Transfer Addendum, as amended to operate for transfers subject to UK GDPR, including:

(i) **Clause 13 (Supervision) and Annex 1.C**: The competent supervisory authority is the UK ICO:

(ii) **Clause 17 (Governing law):** The governing law shall be the laws of England and Wales; and

(iii) **Clause 18 (Choice of forum and jurisdiction):** Disputes shall be resolved by the courts of England and Wales.

2.2 To the extent Supplier (as Data Sender) and Customer (as Data Recipient) enter into UK Controller-Processor Model Contract pursuant to Clause 13.3 of this DP Annex, the UK Controller-Processor Model Contract is amended as follows:

(a) the Security Measures specify the technical and organisational measures to be implemented by the “data importer” and any additional safeguards that must be met in relation to the international transfer and processing of special category personal data are set out in Appendix 1 (if applicable);

(b) Appendix 1specifies:

(iii) the Data Sender(s) acting as the "data exporter(s)";

(iv) the Data Recipient(s) acting as the "data importers(s)";

(v) the activities of each of the "data importer(s)" and "data exporter(s)" and the purposes for which each uses the personal data being transferred;

(vi) the categories of data subject whose personal data is transferred;

(vii) the categories of Personal Data transferred (including special category data);

(viii) the processing operations to which the Personal Data transferred will be subject; and

(b) Clause 9 shall be amended to read: "The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established, namely England".

APPENDIX 4

COUNTRY SPECIFIC ADDENDUM

1. **Switzerland**

(c) In order to ensure that the international transfer under the EU Model Contract is consistent with the Swiss Federal Data Protection Act (**FDPA**), the EU Model Contract is amended in accordance with the below provided that none of these amendments will have the effect or be construed to amend the EU Model Contract in relation to the processing of Personal Data under the GDPR.

(d) In relation to Personal Data that is processed in and exported from Switzerland by Data Sender,

(i) references to a "member state" or to the "EU" in the EU Model Contract will be deemed to include Switzerland;

(ii) references to the GDPR will be deemed to be references to equivalent provisions of the FDPA;

(iii) where the FDPA protects legal entities as data subjects, the EU Model Contract will apply to data relating to identified or identifiable legal entities; and

(iv) the Swiss Federal Data Protection and Information Commissioner will be the sole or, where both the FDPA and the GDPR apply to such transfer, will be one of the competent data protection authorities, under the EU Model Contract.

HOTTINGER BRUEL & KJAER UK LTD
14th of January 2025