DATA PROCESSING ADDENDUM

Last Updated: August 22, 2025

This Data Processing Addendum (the "**Addendum**" or "**DPA**") is incorporated into and forms a part of the Master Subscription Agreement or other similar agreement for Services provided by Processor to Controller (the "**Agreement**") (each term as defined below) which expressly references this DPA. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency. This DPA supersedes and replaces any prior Data Processing Addendum or other similar data privacy or data protection agreement entered into between Controller and Processor in connection with the Agreement.

1. Definitions.

"**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

"**Controller**" is the party that determines the purposes and means of Processing of Personal Data. For purposes of this Addendum, Controller is the party identified on the signature page below and identified in the Agreement as Customer and its Affiliates (if applicable).

"**Data Protection Laws**" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including the GDPR, the UK GDPR and US Privacy Laws, as applicable.

"**Data Subject**" means an identified or identifiable natural person to whom the Personal Data relates. For purposes of this definition, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"**Personal Data** " means any information relating to a Data Subject.

"**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as 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.

"**Processor**" is the party which alone or jointly with others, Processes Personal Data on behalf of Controller. For purposes of this Addendum, Processor is the HighRadius legal entity identified on the signature page below.

"**Services**" means the services provided by Processor to Controller under or in connection with the Agreement.

"**Subprocessing**" means the engagement by Processor of any other person or entity to Process Controller Personal Data on its behalf.

"**UK GDPR**" means the United Kingdom General Data Protection Regulation.

"**US Privacy Laws**" all laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("**CCPA**"), and the Texas Data Privacy and Security Act.

2. **Controller Responsibilities.** Controller shall, in its use of the Services, Process Personal Data in accordance with the requirements of applicable Data Protection Laws and shall ensure that its instructions for Processing of Personal Data are compliant with applicable such Data Protection Laws and all other applicable laws. If Controller issues instructions orally, Controller shall promptly confirm such oral instructions in writing. Processor and its Affiliates shall not be liable for any claim made by a Data Subject arising from or related to Processor's or any of its Affiliates' acts or omissions to the extent that Processor was acting in accordance with Controller's instructions.

3. **Processor Responsibilities.**

3.1 Processor will not Process any Personal Data on behalf of Controller except upon its documented instructions and consistent with the stated Nature and Purpose of the Processing (as set forth in the attached Appendix A), or as required by applicable law and following reasonable notice to Controller (where legally permitted). Controller hereby instructs Processor to Process Personal Data to provide Services in accordance with the Agreement and this DPA.

3.2 Processor shall inform Controller immediately if Processor has a good faith belief that an instruction violates GDPR or other applicable law. Processor shall then be entitled to suspend execution of the relevant instructions until Controller confirms or changes them to comply with applicable law.

4. **Data Transfers by Processor and Adequate Protections.**

4.1 Processor's processing of Controller Personal Data is carried out exclusively within the United Kingdom ("**UK**"), a Member State of the European Union ("**EU**") or within a Member State of the European Economic Area ("**EEA**") except as set forth in this section. Any transfer by Processor of Controller Personal Data to a state that is not the UK, a Member State of either the EU or the EEA shall occur only if the specific conditions of Article 44 *et seq* GDPR or the UK GDPR, as applicable, have been fulfilled.

4.2 Authorized Transfers of Personal Data. Controller approves the transfer of its Personal Data to the following countries outside of UK and the EEA: the United States and India.

4.3 Standard Contractual Clauses. If applicable, Controller and Processor hereby agree to the Standard Contractual Clauses set forth in Appendix C to this DPA in respect of Processor's Processing of Controller Personal Data which is subject to the GDPR and to the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses set forth in Appendix D to this DPA in respect of Processor's Processing of Controller Personal Data which is subject to the UK GDPR.

5. **Protecting Personal Data: Technical and Organizational Measures.**

5.1 With regard to any Controller Personal Data and pursuant to the terms of the attached Appendix B, Processor must maintain and apply appropriate and documented Technical and Organizational Measures to provide a protection level appropriate to the risk concerning confidentiality, integrity, availability, and resilience of its systems, taking into account the state of the art, implementation costs, the nature, scope, and purposes of processing, and

the probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 of the GDPR.

5.2 Accounting for technical advancement, it is permissible for the Processor to implement alternative adequate measures; however, the security level of the defined measures must not be reduced, and substantial changes must be documented.

6. Audit

6.1 Processor has obtained a SOC 2, Type II report ("**SOC 2 Report**") and will continue to obtain annual SOC 2 Reports for the duration of this Addendum. Upon written request from Controller, Processor shall provide a copy of the latest SOC 2 Report to demonstrate Processor's compliance with its obligations under this Addendum. Controller shall accept the findings of such SOC 2 Report with respect to the areas covered by such SOC 2 Report in lieu of conducting an audit in accordance with Sections 6.2 or 6.3 below, as applicable.

6.2 In the event the SOC 2 Report reveals non-compliance with this Addendum or Controller requests to review a control not covered by the SOC 2 Report, Controller may request a virtual audit via a video conferencing platform agreed between the parties ("**Virtual Audit**"). Such a Virtual Audit shall only cover the underlying non-compliant area identified by the Audit Report or the control(s) not covered by the SOC 2 Report.

6.3 Controller may conduct, either itself or through a third-party independent vendor selected by Controller, at Controller's expense, an on-site audit and review of Processor's systems, infrastructure, policies and procedures to the extent reasonably necessary to demonstrate compliance with this Addendum (an "**On-Site Audit**") when: (i) the information available to Controller pursuant to Sections 6.1 and 6.2 (if applicable) is not sufficient to demonstrate Processor's compliance with this Addendum; (ii) a Data Incident has occurred; or (iii) such an On-Site Audit is required by applicable Data Protection Laws or by Controller's supervisory or regulatory authority.

6.4 A Virtual Audit and an On-Site Audit (each, an "**Audit**") may be conducted once every twelve months, upon at least 60 days prior written notice, at a time mutually agreed by the parties unless more frequent audits are required by Data Protection Laws or by any supervisory authority with authority to audit Controller. The scope of the Audits must be mutually agreed between Processor and Controller and any On-Site Audit will be subject to Processor's site access policies and procedures. Any Audit must be limited to no more than two (2) consecutive business days and shall not unreasonably disrupt Processor's business operations.

6.5 Controller acknowledges that all information obtained in connection with this Section shall constitute Processor Confidential Information, and Controller will protect such information in accordance with confidentiality provisions of the Agreement and this Addendum. If Controller conducts an Audit through a third-party independent vendor, such third-party will be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect the Processor's Confidential Information.

7. Data Subject Rights.

7.1 Processor will rectify, erase, or restrict the Processing of data that is being Processed on behalf of Controller on Controller's documented instructions to the extent Controller is unable to do it on his account.

7.2 To the extent legally permitted, if a Controller Data Subject contacts Processor directly concerning a rectification, erasure, or restriction of Processing, Processor will immediately, and in all cases within five (5) business days, forward the Data Subject's request to Controller.

7.3 Processor will assist Controller in fulfilling Data Subject requests to exercise rights of rectification, erasure, restriction, objection, data portability, or access in accordance with

documented instructions from Controller without undue delay to the extent commercially practicable. Processor may charge a reasonable fee to assist Controller in the fulfilling of its obligations under this Addendum.

8. Subprocessing.

8.1 Processor shall ensure that any person or entity it engages to perform Subprocessing (a "**Subprocessor**") is legally bound in writing to data protection obligations substantially similar to those in this Addendum with respect to the protection of Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. Processor shall remain fully liable to Controller for the performance of all obligations subcontracted to its Subprocessors in accordance with the terms of the Agreement.

8.2 Controller authorizes Processor to engage the Subprocessors listed on the website www.highradius.com/subprocessors/ to Process the Controller Personal Data provided that (i) such list include the name and location of the Subprocessor and a short description of the Subprocessing activity to be performed, (ii) Processor updates such list with any change in Subprocessors at least thirty (30) days' prior to any such change and (iii) such website provides a mechanism for Controller to be notified of any updates to such list (such as through a RSS feed or email subscription). Within fourteen (14) days of publication to the above website, Controller may object in writing to Processor's appointment or replacement of a Subprocessor that is not an Affiliate of Processor, provided such objection includes Controller's reasons therefor that are based on reasonable grounds relating to data protection. In the event of a timely objection, if Processor is unable to address Controller's objection to its reasonable satisfaction within 30 days, Processor shall, at its sole discretion, either (i) not appoint or replace the Subprocessor with respect to Controller or (ii) permit Controller to terminate the affected Services without penalty, it being understood and agreed that such right of termination is Controller's sole and exclusive remedy if Controller objects to any new or replacement Subprocessor.

8.3 As of the date of this Addendum, Controller authorizes Processor to engage the following Subprocessors:

Processor and its Affiliates:

Name	Address/Country	Sub-processing activity
HighRadius Corporation	2107 CityWest Blvd, Suite 1100, Houston, TX 77042 USA	Implementation, development, and support activities
HighRadius UK Limited	Heron Tower 110 Bishopsgate London EC2N 4AY United Kingdom	Implementation and support activities
HighRadius B.V.	EDGE Workspaces Olympic Fred. Roeskestraat 115, 1076 EE Amsterdam, Netherlands	Implementation and support activities
HighRadius GmbH	Rathenauplatz 1A, 60313 Frankfurt am Main, Germany	Implementation and support activities
HighRadius SAS	3-5 rue Saint-Georges 75009 Paris, France	Implementation and support activities
HighRadius Technologies Private Limited	Highradius Technologies Private Limited	Implementation, development, and support activities

	Hyderabad Office: 1st Floor, Building No: 12C, Mindspace, Hitech City, Madhapur, Ranga Reddy District, Hyderabad, Telangana, PIN-500081, India	

Third-party Subprocessors:

Name	Address/Country	Sub-processing activity	Applicable HighRadius Cloud Solution
Amazon Web Services, Inc.	Business Address: 410 Terry Avenue North, Seattle, WA 98109-5210, USA Data Centers: USA, Europe (Germany, Ireland)	Cloud infrastructure, hosting and related services (including Amazon Bedrock[1])	All
Google LLC and its affiliates	Business Address: 1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA Data Centers: USA, Canada, Europe	Google Workspace / G-Suite / Gmail used to process data which the HighRadius cash application cloud solution reads and captures Google Cloud Platform cloud infrastructure, hosting and related services (including Vertex AI[2])	All
Microsoft Corporation	Business Address: One Microsoft Way, Redmond, WA 98052, U.S.A. Washington State Data Centers: USA, Europe (Germany, Ireland)	Azure cloud infrastructure, hosting and related services (including Azure OpenAI Service[3])	All
Pendo.io, Inc.	Business Address: 150 Fayetteville Street, Suite 1400 Raleigh, NC 27601, USA Data Centers: USA	Insights and analytics on usage of the HighRadius cloud services by customers	All

[1] https://aws.amazon.com/bedrock/security-compliance/
[2] https://cloud.google.com/vertex-ai/generative-ai/docs/data-governance
[3] https://learn.microsoft.com/en-us/azure/ai-foundry/responsible-ai/openai/data-privacy?tabs=azure-portal

SalesForce, Inc.	Business Address: Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA Data Centers: USA	Service Cloud - IT service management / ticketing tool for technical support	All
Snowflake Inc.	450 Concar Drive, San Mateo, CA, 94402, USA Data Centers: USA, EU	Data warehousing to support higher performance and advanced data analysis.	All
Twilio Inc.	375 Beale Street, Suite 300, San Francisco, CA 94105, USA	Voice-over internet protocol services for voice communications in certain HighRadius cloud services.	Autonomous Collections
Data B.V. (Storecove)	s-Gravelandseweg 46-D 1211BT, Hilversuym, The Netherlands Data Centers: Ireland	E-invoicing services to multiple government authorized invoice networks.	Electronic Invoicing Payment and Presentment (EIPP)

9. **Assistance with Controller Obligations.** Processor shall, to the extent applicable and provided that Controller cannot reasonably perform the following independently with information available to the Controller:

   9.1 Assist Controller with its obligation to provide information to the relevant Data Subject by promptly providing Controller with all relevant information to the extent practicable;

   9.2 Assist Controller with a data protection impact assessment; and

   9.3 Assist Controller with regard to consultation of a supervisory authority.

10. **Data Incidents and Notification.** If Processor becomes aware of any unauthorized or unlawful access to or destruction, loss, disclosure or modification of Controller Personal Data by a third party (a "**Data Incident**"), Processor will notify Controller of such Data Incident without undue delay and take all action as may be necessary to preserve forensic evidence and to mitigate the cause of such Data Incident. Processor will provide Controller with information necessary for Controller to understand the nature and scope of the Data Incident. Processor will provide Controller with information about what Processor has done or plans to do to mitigate the effects of the Data Incident. Controller will be responsible for (a) determining if there is any notification or other obligation applicable to Controller under applicable Data Protection Laws and (b) taking necessary action to comply with those Controller obligations; provided that Controller shall use commercially reasonable efforts to consult with Processor at least 24 hours prior to disclosure of a Data Incident.

11. **Deletion and Return of Personal Data.**

   11.1 Processor may not create copies or duplicates of the Controller Personal Data without Controller's knowledge and consent, except (i) as required to provide Services, (ii) for back-up copies to the extent necessary to ensure orderly data processing and disaster recovery, or (iii) to the extent required by applicable law or regulatory requirements to retain data.

11.2 Upon Controller's written request within 30 days after termination or expiration of the Agreement, Processor will make Controller Personal Data available to Controller in an industry standard format. After such 30-day period, Processor has no obligation to maintain the Customer Data and will destroy it; provided that Processor may maintain the Customer Data to the extent required for legitimate business purposes, including to comply with legal obligations, resolve disputes and conduct audits.

12. Liability Limits. Each party's liability arising out of or related to this DPA is subject to the "*Liability Limits*" (or similar limitations of liability) section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and its Affiliates under the Agreement and this DPA.

13. California Consumer Privacy Act. The following provisions are applicable if the CCPA applies to the Processing of Personal Data under the Agreement.

13.1 CCPA Definitions.

"**Business Purpose**" shall have the meaning set forth in the CPRA.

"**CCPA**" means the California Consumer Privacy Act of 2018 which governs the use of California residents' Personal Data as amended by the CPRA.

"**Consumer**" shall have meaning as defined under the CCPA.

"**CPRA**" means the California Privacy Rights Act of 2020.

"**Cross-Context Behavioral Advertising**" means the targeting of advertising to a Consumer based on the Consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

"**Reasonable Security Procedures and Practices**" means security measures appropriate to the nature of the Personal Information that are implemented and maintained to prevent the unauthorized access and exfiltration, theft, or disclosure of nonencrypted or nonredacted Personal Information.

"**Security Breach**" means the unauthorized access and exfiltration, theft, or disclosure of a Consumer's nonencrypted and nonredacted Personal Information, resulting from a violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

"**Sale of Data**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Consumer's Personal Data by a business to another business or a third party for monetary or other valuable consideration.

13.2 Amendments to Definitions.

The definition of "**Controller**" includes "Business" as defined under the CCPA.

The definition of "**Data Incident**" includes "Security Breach".

The definition of "**Data Subject**" includes "Consumer" as defined under the CCPA.

The definition of "**Personal Data**" includes "Personal Information" as defined under the CCPA.

The definition of "**Processor**" includes "Service Provider" as defined under the CCPA.

13.3 CCPA Obligations.

13.3.1 Processor will not Process any Personal Data on behalf of Controller except consistent with the stated nature and purpose of the Processing (as set forth in the attached Appendix A), which the parties agree constitutes a Business Purpose.

13.3.2 Processor will not engage in the Sale of Data unless otherwise permitted under the Agreement or the DPA without the prior express written consent of Controller, and, when required, the persons to whom such Personal Data relates.

13.3.3 Processor will maintain the Technical and Organizational Security Measures in Appendix B, which the parties agree constitute Reasonable Security Procedures and Practices.

13.3.4 Processor will not use any Personal Data it receives from Controller for Cross-Context Behavioral Advertising.

13.3.5 Processor shall provide reasonable assistance to Controller for the fulfilment of Controller's obligation to respond to and address requests of Consumers relating to rights provided by CCPA provided that Controller cannot reasonably perform fulfil such obligation independently with information available to the Controller. Controller shall be responsible for any costs arising from Processor's provision of such assistance. Processor shall not be required to delete any of the Personal Data to comply with a request to exercise CCPA rights directed by Controller if it is necessary to maintain such information in accordance with Cal. Civ. Code 1798.105(d), in which case Processor shall promptly inform Controller of the exceptions relied upon under Cal. Civ. Code 1798.105(d) and Processor shall not use the Personal Data retained for any other purpose than provided for by that exception.

Appendix A to Data Processing Addendum
Processor & Processing Information

This Appendix A includes certain details of the processing of Controller Personal Data by Processor and is incorporated into the Data Privacy Addendum between Controller and Processor.

1. **Subject matter of processing of Controller's Personal Data by Processor.** The subject matter of the Processing of Controller Personal Data is the software as a service ("**SaaS**") and related services provided by Processor to Controller pursuant to the terms and conditions of the Agreement.

2. **Duration of processing.**

   The Duration of processing is during the term of the Agreement and for limited periods thereafter as specifically contemplated under the Agreement.

3. **The nature and purpose of the processing of Controller's Personal Data by Processor.** The nature and purpose of the Processing of Controller Personal Data are the following:

   3.1 Processor providing the SaaS Services to Controller as contemplated under the Agreement;

   3.2 Use of Personal Data to provide updates to the software and Services and to provide assistance and technical support in connection with the software and Services;

   3.3 Storage and backup of Personal Data in data centers;

   3.4 Computer processing of Personal Data, including data transmissions, data retrieval and data access;

   3.5 Network access to all Personal Data transfers; and

   3.6 Use of Personal Data to provide IT services, including software licensing and implementation, whether on-premises or as a SaaS solution, regarding the administration and facilitation of essential business processes.

4. **The types of Controller Personal Data to be Processed by Processor.** The Personal Data transferred by Controller to Processor concerns the following categories of data:

   4.1 Name, address, phone/fax number, email address, system details (e.g. IP address, operating system and browser information), job location, title/position/role/job description, payment information (e.g. account numbers, routing numbers and cheque details), insurance policy number, tax ID and any other information that may be used or combined with other information to identify an individual.

5. **The categories of data subjects.** The Personal Data transferred by Controller to Processor concerns the following categories of data subjects:

   5.1 Customers (of Controller);

   5.2 Employees, contractors or representatives of Controller; and

   5.3 Employees, contractors or representatives of Controller's customers, partners, and suppliers.

Appendix B to Data Processing Addendum
Technical and Organizational Measures

This Appendix B is incorporated into the Data Privacy Addendum between Controller and Processor.

1. Information Security Policies

Processor has written policies describing the technical and organizational measures implemented for information security. The security policies consider the real risks the Personal Data are exposed to. They include a description of how to manage security incidents, a description of the awareness-raising process for the policies within the organization and a description of the various responsibilities and organizational rules.

The security policies have been approved by the relevant persons in the organization and have been adequately disseminated within the organization. A reassessment of these technical and organizational measures is performed on a regular basis in order to ensure that the goals and the measures taken remain up-to-date so that improvements can be made if necessary. Security controls are updated in the event of any reorganization or modification of infrastructure. The security policies will be adapted where necessary as a result of modifications or reassessment.

Processor has appointed a Head of Information Security, who oversees the implementation of the security policies. The Head of Information Security possesses the necessary competences, is adequately trained and will not be able to discharge any function or take up any responsibility that is incompatible with that of a Head of Information Security.

2. Organization and Human Aspects of Security

Policies on information security have been disseminated within the organization and training has been regularly conducted to ensure that all employees participating in the Processing of Personal Data are sufficiently informed about their duties and responsibilities during Processing operations.

Processor's employees are bound by legally enforceable confidentiality obligations to Processor.

3. Access Control to Premises

Processor has implemented the following measures to prevent unauthorized access to the premises on which the Personal Data is Processed:

- Processor premises and the third-party data centers in which the Personal Data is Processed are equipped with industry-standard security measures and follow industry "Best Practices", including electronic access control systems by key card, alarm systems, cameras for the interior and the exterior, and security staff.
- Processor does not provide access to the third-party data centers in which the Personal Data is Processed. Independent audits are conducted by third-party auditors on the controls and security systems of the third-party data centers on an annual basis, and Processor receives and reviews each independent audit report.
- Authorized visitors to Processor premises are provided with temporary identity cards and need to be accompanied by an authorized employee of Processor to gain access to sensitive areas. Records of visitors are made.

4. Access Control to Systems and Data

Processor takes the following measures to prevent the unauthorized use of systems by which Personal Data is Processed:

- Secured access connections using virtual private networking and technologies for authentication control are implemented to regulate the access to Processor's systems and internal support-tools.
- Encryption is used to secure user authentications.
- Processor follows a formal process to restrict the access to Processor resources. Unique login names, strong passwords and periodic examinations of the access lists are required to ensure the appropriate use of user accounts. All groups which have access to Processor services are controlled by a regular examination.

5. Access Authority Control

Processor ensures that (i) authorized users who have access to the data processing systems can only access Personal Data within their Processing authorization and (ii) the unauthorized reading, change or deletion of Personal Data is prohibited during Processing or after the storing of Personal Data.

The access rights are granted based on the job responsibilities of the user and on a need-to-know basis and must be authorized and granted by the corresponding supervisor of the user and, for sensitive data, by the information security team as well. The access to production systems is only granted to users who are periodically trained and authorized. The access to production systems is also immediately withdrawn upon termination of employment or assignment of the user to a different job responsibility without the need for such access.

6. Disclosure Control

Processor takes the following measures to ensure that Personal Data is not read, altered or removed without authorization during transmission, storage or Processing:

- The remote access to data on Processor's production machines requires a connection to Processor's network, which requires double authentication for access via virtual private networking.
- The transmission of Personal Data to and from Processor's network is secured by generally accepted security and encryption technologies.
- Personal Data is stored encrypted at rest using generally accepted security and encryption technologies.
- The data processing systems are protected against the risk of intrusion with the help of suitable software and hardware whose effectiveness and updating is checked periodically. The routers are appropriately configured to secure Processor's internal network from unauthorized external connections and to ensure that network connections and data flows do not breach the logical access adjustment control of Processor's systems. Modifications on the hardware-based network components or on their configurations require the approval of the designated responsible person and are subject to a change management process.
- Processor has a firewall configuration rule which defines acceptable ports. Only used ports and services are open. The access for the modification of the firewall configuration is restricted to an internal team of security experts. Such team regularly examines critical firewall rules.
- Processor has policies in place governing the secure disposal of storage media and devices containing Personal Data.

7. Input Control

Processor takes the following measures to guarantee that it can subsequently examine and determine if and by whom Personal Data have been entered into data processing systems, altered or removed:

- Effective input control is applied to ensure that Personal Data cannot be read or modified without authorization in the course of Processing and after storage. All access requests are logged, and their compliance is monitored.

8. Job Control

Processor takes the following measures to guarantee that the Processing of Personal Data is made in correspondence with the Controller's instructions:

- The Processing to be performed by Processor is clearly defined, updated and documented on applicable written Order Forms and Statements of Work.

9. Availability Control

Processor takes the following measures to guarantee that Personal Data is protected against damage by accident or loss:

- Personal Data is protected from accidental destruction or loss through effective retrieval systems, disaster recovery and business continuity planning. The procedures laid down for making backup copies and for recovering data ensure that data can be reconstructed in the state they were at the time they were last backed up.

10. Security Incident and Continuity Management

The security policies describe the steps to be taken when a security incident relating to Personal Data is detected, as well as of the person(s) responsible for resolving the incident as quickly as possible.

The procedure for reporting and managing security incidents includes a record of each incident, the time at which it occurred, the person reporting it, to whom it was reported and the effects thereof. The circumstances of any incident are to be analysed in order to develop preventive measures or make modifications to avoid a repeat of a similar incident.

11. Segregation Control

Processor undertakes the following measures to separate the Processing of Personal Data:

- Data Processing for different controllers is made on server systems which are separated by a system of logical and physical access controls in the network as required such that each controller only has access to its own data.

12. Documentation

Processor has documentation relating to information security, which is proportional to Processor's information security needs and is regularly maintained. Such documentation includes the following elements: the identity of the Head of Information Security, the security policies, the implementation of security measures, a record of the types of Personal Data being Processed and the operations performed on them, a list of persons having access to the data, the system and network configuration, technical documentation about the security controls that were introduced, a schedule of planned operations, the incident management policy, security control test plans, incident reports, and audit reports, if any.

Appendix C to Data Processing Addendum

EU STANDARD CONTRACTUAL CLAUSES

(Module 2 – Controller to Processor)

SECTION I

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

b. The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7; Clause 8.1(b), 8.9(a), (c), (d) and (e);

ii. Clause 9(a), (c), (d) and (e);

iii. Clause 12(a), (d) and (f);

iv. Clause 13;

v. Clause 15.1(c), (d) and (e);

vi. Clause 16(e);

vii. Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

1. Instructions
    a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
    b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

2. Purpose limitation

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

3. Transparency

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

4. Accuracy

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

5. Duration of processing and erasure or return of data

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

6. Security of processing

    a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of

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

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

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

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

7. Sensitive data

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

8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

9. Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-

processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

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

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

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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

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

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

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

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

Clause 15

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

1. Notification

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

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

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

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

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

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

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

2. Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii. the data importer is in substantial or persistent breach of these Clauses; or

iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18
Choice of forum and jurisdiction

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

b. The Parties agree that those shall be the courts of the Netherlands.

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

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

ANNEX I

A. **LIST OF PARTIES**
Data exporter(s):

The "Controller" as defined in the DPA.

Activities relevant to the data transferred under these Clauses:

For receipt of the software as a service ("SaaS") and related services provided by Processor to Controller pursuant to the terms and conditions of the Agreement.

Role (controller/processor): Controller

Data importer(s):

The "Processor" as defined in the DPA

Activities relevant to the data transferred under these Clauses:

For delivery of the software as a service ("SaaS") and related services provided by Processor to Controller pursuant to the terms and conditions of the Agreement.

Role (controller/processor): Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

The data subjects are those identified in the Agreement and the DPA.

Categories of personal data transferred

The personal data transferred concern those categories of data identified in the Agreement and the DPA.

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.

Not applicable.

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

Continuous

Nature of the processing

The personal data transferred will be subject to the processing activities identified in the Agreement and the DPA.

Purpose(s) of the data transfer and further processing

For delivery of the software as a service ("SaaS") and related services provided by Processor to Controller pursuant to the terms and conditions of the Agreement.

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

The Duration of processing is during the term of the Agreement and for limited periods thereafter as specifically contemplated under the Agreement.

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

Same as Processor.

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13
Dutch Data Protection Authority
Autoriteit Persoonsgegevens
PO Box 93374
2509 AJ DEN HAAG

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Processor will maintain technical and organisational security measures as described in Appendix B to the Data Processing Addendum.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors as described in Section 8.3 of the Data Processing Addendum.

Appendix D to Data Processing Addendum

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

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date	The date of the DPA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The "Controller" as defined in the DPA	The "Processor" as defined in the DPA
Key Contact	See signature section of DPA, the Agreement or Order Form	See signature section of DPA, the Agreement or Order Form

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to is attached as Appendix C to the DPA

Table 3: Appendix Information

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

Annex 1A: List of Parties: See Table 1 above
Annex 1B: Description of Transfer: See Appendix A to the DPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Appendix _B to the DPA
Annex III: List of Sub processors (Modules 2 and 3 only): See Section 7.3 to the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

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

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

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

Hierarchy

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

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides

greater protection for data subjects, in which case those terms will override the Approved Addendum.

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

Incorporation of and changes to the EU SCCs

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

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

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

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

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

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

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

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

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

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

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

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

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

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

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

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

<u>Amendments to this Addendum</u>

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

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

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

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

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

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

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

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

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