INSTRUCTIONS FOR EXECUTING THIS FRAMEWORK DATA PROCESSING AGREEMENT

This Framework Data Processing Agreement has been pre-signed on behalf of Siemens.

To fully execute this Framework Data Processing Agreement, the Customer must:

1. complete the customer information on Page 1 and sign on Page 3; and

2. submit the completed and fully executed Framework Data Processing Agreement without any changes to the printed terms to Siemens via dataprivacy.func@siemens-healthineers.com.

Upon receipt by Siemens of a fully completed and duly executed Framework Data Processing Agreement, this Framework Agreement shall become legally binding.

Framework Agreement
regarding
Data Processing
as defined under Article 28 GDPR

between

please complete

- hereinafter referred to as the "Customer" -

and

Siemens Healthcare GmbH

Henkestr. 127, 91052 Erlangen

- hereinafter referred to as the "Siemens" -

- hereinafter referred to individually as the “Party” or collectively as the “Parties” -

Preamble

The Parties are aware of the importance of protecting the right to privacy and are aware of the existing privacy laws and regulations. This Framework Agreement specifies in detail the data protection obligations of the Parties arising from existing or future contracts for e.g. deliveries and services, insofar as these relate to the processing of personal data of the Customer or his customers, particularly within the meaning of the EU-General Data Protection Regulation (GDPR).

Article 1 - Subject Matter of this Framework Agreement

This Framework Agreement applies to all data processing services as per Art. 28 GDPR that are provided for the Customer by Siemens on the basis of main contracts (e.g. delivery, service, installation), in particular all activities in which employees of Siemens or sub-processors ("another processor") engaged by Siemens may have access to the Customer's personal data or that of third parties.

The provisions of this Framework Agreement take precedence over any provisions in individual contracts. Specific provisions deviating from this Framework Agreement take precedence over this Framework Agreement only if they expressly refer to this Framework Agreement.

Article 2 - Specification of the Subject Matter of Data Processing

The specific description of the subject matter, nature, purpose and duration of Siemens' processing of personal data by Siemens for the Customer is contained in the existing and future main contracts within the meaning of Article 1.

Article 3 - Data Privacy Specific Regulations

The data privacy specific regulations applicable to Siemens' activities are set out in the Siemens Healthineers Data Processing Agreement (Annex DPA) applied as amended.

Article 4 - Term and Termination

This Framework Agreement comes into force upon signature by both Parties and initially applies for a period of 36 months. The term shall then be extended by 12 months in each case, provided that this Framework Agreement is not terminated by one of the two Parties 3 months prior to the expiry of the term of this Framework Agreement. The right to terminate the contract for good cause remains unaffected. If this Framework Agreement ends, the term and termination conditions of the main contract which the Annex DPA supplements apply.

Article 5 - Miscellaneous

Any cancellation, amendment and addition to this Framework Agreement must be made in writing in order to be valid. A waiver of form is effective only if agreed upon in writing.

If individual provisions of this Framework Agreement are or become invalid in full or in part or can no longer be executed in the intended manner for legal reasons, this does not affect the validity of the rest of this Framework Agreement. The Parties shall rather work together to establish a regulation in place of the invalid provision that is suitable to achieve the intended outcome of the invalid provision.

Annex DPA: Siemens Healthineers Data Processing Agreement according to Article 28 GDPR (DPA)

[Customer]

Place, date:	Place, date:
______________________________	______________________________
Name:	Name:
______________________________ (printed)	______________________________ (printed)
Title:	Title:
______________________________	______________________________

Siemens Healthcare GmbH

Place, date:	Place, date:
Erlangen, 01 May 2019	Erlangen, 01 May 2019
Name:	Name:
Dr. Stefan Schaller	Ashraf Baig
Title:	Title:
Head of Siemens Germany Healthcare	Commercial Director Siemens Germany Healthcare

Annex DPA: Siemens Healthineers Data Processing Agreement according to Article 28 GDPR (DPA)

This DPA supplements and specifies the data protection obligations of the main contract concluded between the parties. This DPA applies to all activities related to the main contract in which employees of Siemens or third parties contracted by Siemens process personal data of the Customer or his clients.

Article 1 Subject-matter, nature, purpose and duration of the processing

(1) This DPA supplements the main contract concluded between the parties. It applies to the processing of personal data by Siemens (the "Processor") on behalf of the Customer (the "Controller") under the main contract and sets out the data protection obligations of the parties.

(2) Nature and purpose of the processing: Siemens processes personal data to the extent necessary to provide the services specified and agreed to in the main contract.

(3) Siemens and the Customer are each responsible for their own compliance with the applicable data protection law. The Customer is solely responsible for the means by which the Customer acquired the personal data and the Customer shall only disclose personal data to Siemens for which a legal authorization is given and for which the Customer has a legal right of processing.

(4) The duration of the processing corresponds to the term of the main contract.

Article 2 Type of personal data and categories of data subjects

Depending on the provisions of the main contract, the categories of data subjects are in particular employees, patients, contact persons of the Customer and contractual partners of the Customer. The types of personal data included in the processing are in particular contact information, identifiers, health information, genetic data, biometric data, location data and financial information.

Article 3 Instructions

(1) Siemens processes personal data only on the basis of the Customer's documented instructions. This DPA and the main contract are the Customer's complete and final documented instructions to Siemens for the processing of personal data.

(2) Any additional or alternate instructions must be issued by the Customer in writing and are binding only upon written acknowledgement by Siemens. Siemens shall inform the Customer if, in Siemens' opinion, an instruction infringes the GDPR or the data protection provisions applicable to Siemens as data processor. Siemens is under no obligation to conduct a comprehensive legal review or to follow instructions prohibited by law.

(3) The Customer shall bear all additional costs incurred by Siemens as a result of an additional or alternate instruction, unless the instruction is necessary to comply with statutory requirements applicable to Siemens.

Article 4 Confidentiality

Siemens warrants that persons authorized to process the personal data are bound to continuing secrecy by contract or are under such a duty by law.

Article 5 Security of processing

(1) Siemens shall take all measures required pursuant to Article 32 GDPR.

(2) 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, and in particular the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed, Siemens shall implement technical and organizational measures with a level of protection at least equal to that set out in **Attachment TOM**.

(3) The Customer and Siemens agree that the implementation of the technical and organizational measures described in **Attachment TOM** ensures an appropriate level of security in accordance with the GDPR and provides sufficient safeguards for the protection of the rights of the data subject.

(4) The technical and organizational measures described in **Attachment TOM** are subject to technical progress and further development and may be adjusted by Siemens if appropriate, provided such adjustment does not result in a lower level of protection than that set forth in **Attachment TOM**.

Article 6 Sub-processors

(1) Siemens engages sub-processors (another processor) to carry out specific processing activities on behalf of the Customer. Sub-processors are only allowed to process personal data for the purpose of carrying out the activities for which such personal data have been provided to Siemens and are prohibited from processing personal data for other purposes. If Siemens engages sub-processors, they will be subject to written data protection obligations, providing at least the same level of protection as set forth in this DPA. Siemens shall in particular provide sufficient safeguards that the appropriate technical and organizational measures are implemented in such a way that processing meets the requirements of the GDPR, ensure the protection of the rights of the data subjects concerned, maintain a record of data transfers and document suitable safeguards.

(2) A list of sub-processors currently engaged by Siemens is available at https://siemens.com/LifeNet. Siemens reserves the right to update this URL from time to time. The Customer hereby authorizes Siemens to engage the listed companies as sub-processors. The Customer shall subscribe to this Siemens' website to receive the information regarding sub-processors and for any intended changes in the use or replacement of sub-processors.

(3) The engagement or replacement of an additional sub-processor shall be deemed approved if Siemens informs the Customer in advance thereof and the Customer raises no objection to Siemens in writing, including in electronic form, within 1 month following such information.

(4) If the Customer objects the Customer shall notify Siemens in detail about the reasons for the objection.
Following an objection, Siemens may at its discretion

a. propose another sub-processor in place of the rejected sub-processor; or
b. take steps to address the concerns raised by the Customer which remove the Customer’s objection.

(5) If the options as per this Article 6 (4) a. and b. are reasonably not available or the objection has not been removed otherwise, Siemens may terminate the main contract in full or in part without notice, e.g. if the Customer’s objection makes it considerably more difficult or impossible for Siemens to perform its contractual obligations.

(6) Any agreements on response times or availability will be suspended and any claims in this regard for damages in lieu of performance, for delay or for any agreed liquidated damages or contractual penalties with regard to Siemens do not apply from the planned start date of the objected to sub-processor onwards. If Siemens' performance obligations are terminated in part, the remuneration for the services unaffected by the partial termination shall be determined in accordance with Siemens' standard list prices applicable to such services at Siemens.

(7) Where the sub-processor fails to meet its data protection obligations, Siemens shall – in accordance with the provisions on liability in the main contract – remain fully liable to the Customer for the performance of the sub-processor’s obligations. Siemens shall not be liable for damages and claims arising from the Customer’s additional or alternate instructions as per Article 3 (2) of this DPA.

(8) In case Siemens engages a sub-processor in a third country (outside the EU/EEA), Siemens shall use data transfer mechanisms compliant with Articles 44 et seq. GDPR.

(9) In case Siemens provides sufficient safeguards e.g. by standard contractual clauses according to EU Commission decision 2010/87/EU or standard protection clauses according to Article 46 (“standard data protection clauses”), the Customer herewith authorizes Siemens to enter into such standard data protection clauses in the name and for the account of the Customer. Further, the Customer expressly permits Siemens to also represent the respective sub-processor when entering into such standard data protection clauses. This means that Siemens is authorized to act on behalf of the Customer and the sub-processor for establishing standard data protections clauses. Siemens is also entitled to exercise the Customer’s rights and powers under the standard data protection clauses vis-à-vis the sub-processor.

Article 7 Assistance

(1) Taking into account the nature of the processing as described in the main contract and this DPA, Siemens will assist the Customer upon request and at the Customer’s expense by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to requests for exercising the data subject's rights laid down in Articles 12 to 23 GDPR.

(2) Siemens shall inform the Customer without undue delay about requests from data subjects to exercise their rights as per Articles 12 to 23 GDPR, in particular with regard to the right of access to personal data, right to rectification, right to erasure (‘right to be forgotten’), right to restriction of processing, right to data portability, right to object or the right not to be subject to an automated individual decision-making.

(3) Taking into account the nature of the processing as described in the main contract and this DPA and the information available at Siemens, Siemens shall assist the Customer at the Customer's expense in ensuring Customer's own compliance with the obligations pursuant to Articles 32 (security of processing), 33 (notification of personal data breach to the supervisory authority), 34 (communication of a personal data breach to the data subject), 35 (data protection impact assessment) and 36 (prior consultation) GDPR.

Article 8 Deletion

At the choice of the Customer all personal data of the Customer are to be deleted or returned after the end of the provision of services relating to processing. Customer hereby instructs Siemens to delete all personal data of the Customer after the end of the provision of services relating to processing and to delete existing copies unless Union or Member State law requires storage of the personal data.

Article 9 Information and audit rights

(1) With regard to the processing under the main contract, Siemens shall upon the Customer's written request make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

(2) Siemens shall allow for and contribute to Customer audits, including inspections ("Audits"), with regard to the processing under the main contract to demonstrate compliance with the obligations laid down in Article 28 GDPR. These Audits may also be conducted by an independent third party auditor mandated by the Customer, provided that this auditor is acceptable for Siemens and bound by confidentiality obligation no less restrictive than those applicable to the Customer under the main contract. The Customer shall request an Audit with reasonable prior notice to Siemens. Prior to an Audit, the parties shall mutually agree on the scope, timing, and duration of the audit. The Customer shall reimburse Siemens for any services incurred by Siemens with regard to the Audit at the then current Siemens service rates, which shall be made available to the Customer upon request.

(3) The Customer shall promptly provide a written report to Siemens containing a confidential summary of the scope and results of the Audit. Irrespective hereof, Siemens is entitled to use the report for its own purposes.

Attachment TOM:

Technical and Organizational Measures (“Attachment TOM”) Siemens Healthineers

Siemens maintains appropriate technical and organizational measures (Information Security Management System) to ensure a risk-adequate level of security.

1. Pseudonymization and Encryption of Personal Data

Siemens separates personal data from the processed data so that it is not possible to link the processed data to an identified or identifiable person without additional information that is stored separately and securely. Siemens encrypts personal data with symmetric or asymmetric keys.

2. Confidentiality, Integrity, Availability and Resilience of Systems and Services

a) Siemens ensures confidentiality and integrity by taking the following measures:

Access control:
Siemens protects its buildings with appropriate access control systems based on a security classification of the buildings and an appropriately defined access authorization concept. All buildings are secured by access control measures such as a card reader system. Depending on the security level, property, buildings or individual areas are secured with additional measures. These may include special access profiles, biometrics, pin pads, DES dongles, separation locks, video surveillance and security personnel. Access rights for authorized persons are granted individually according to defined criteria. This also applies to external persons.

System access control:
Access to data processing systems is only granted to authenticated users based on a role-based authorization concept using the following measures: Data encryption, individualized password assignment (complex characters, regularly automatic expiration), employee ID cards with encryption, password-protected screen savers in case of inactivity, network intrusion detection systems and intrusion-prevention systems, regularly updated antivirus and spyware filters in the network and on the individual servers and mobile devices.

Data access control:
Access to personal data is granted on the basis of a role-based authorization concept. A user management system has been set up, which maps the user database with their respective authorizations and is available centrally in the network for retrieval by requesting data processing systems. Furthermore, data encryption prevents unauthorized access to personal data.

Data transmission control:
Siemens secures electronic communication channels by setting up closed networks and data encryption procedures. If a physical data carrier transport takes place, verifiable transport processes are implemented that prevent unauthorized data access or logical loss. Data carriers are disposed of in accordance with data protection regulations.

b) Siemens ensures systems and services availability and reliability by taking the following measures:

Siemens ensures availability and resilience of systems and services by isolating critical IT and network components, by providing adequate backup and redundancy systems, using power redundancy systems, and regularly testing of systems and services. Test and live systems are kept completely separated.

3. Availability and Access to Personal Data in the Event of an Incident

Siemens shall restore the availability of and access to personal data in the event of a physical or technical incident.
A comprehensive written emergency plan is available. Emergency processes and systems are regularly reviewed.

4. Control Procedures to ensure the Safety of Processing

Siemens maintains a Security Framework based on a risk-management-based approach, taking into account the basic IT protection catalogues of the Federal Office for Information Security (BSI) and ISO/IEC 27001 requirements for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure security of processing. This ensures the protection of relevant information, applications (including quality and safety test methods), operating environments (e. g. by network monitoring against harmful effects) and the technical implementation of protection concepts (e. g. by means of vulnerability analyses). By systematically detecting and eliminating weak- points, the protective measures are continuously questioned and improved.

5. Personnel Measures

Siemens issues written work instructions and regularly trains personnel who have access to personal data to ensure that personal data is only processed in accordance with the law, this DPA and associated instructions of the Customer, including the technical and organizational measures described herein.