Data Processing Agreement according to Article 28 GDPR (DPA)

(Version: 06.05.2024)

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 Healthineers or third parties contracted by Siemens Healthineers process personal data of the Customer or his clients.

0. Interpretation

0.1. Where this DPA uses the terms defined in the GDPR, those terms shall have the same meaning as in the GDPR.

0.2. This DPA shall be read and interpreted in the light of the provisions of the GDPR.

0.3. This DPA shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

1. Subject-Matter, Nature, Purpose, Purpose Limitation and Duration of the Processing

1.1. This DPA supplements the main contract concluded between the Parties. It applies to the processing of personal data by Siemens Healthineers (the "Processor") on behalf of the Customer (the "Controller") under the main contract and sets out the data protection obligations of the Parties. The specific description of the subject matter, nature, purpose and duration of Siemens Healthineers' processing of personal data by Siemens Healthineers for the Customer is contained in the existing and future main contracts.

1.2. Nature and purpose of the processing: Siemens Healthineers processes personal data to the extent necessary to provide the services specified and agreed to in the main contract. Siemens Healthineers must not process the personal data for other purposes.

1.3. Siemens Healthineers 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 Healthineers for which a legal authorization is given and for which the Customer has a legal right of processing.

1.4. The duration of the processing corresponds to the term of the main contract.

2. Type of Personal Data and Categories of Data Subjects

Depending on the provisions of the main contract, the categories of data subjects whose personal data are processed 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, location data, financial data and sensitive data such as health information, genetic data and biometric data.

3. Instructions

3.1. Siemens Healthineers 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 Healthineers for the processing of personal data.

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

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

4. Confidentiality

Siemens Healthineers shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the main contract. Siemens Healthineers ensures that persons authorized to process the personal data received have committed themselves to continuing confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Security of Processing

5.1. Siemens Healthineers shall take all measures required pursuant to Article 32 GDPR.

5.2. 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 Healthineers shall implement technical and organizational measures as set out in Attachment TOM.

5.3. The Customer and Siemens Healthineers 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.

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

6. Sub-processors

6.1. Siemens Healthineers shall not subcontract any of its processing activities performed without the prior authorization of the Customer. Where Siemens Healthineers subcontracts its processing activities with the authorization 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 Healthineers and are prohibited from processing personal data for other purposes.

Any sub-processor shall be engaged by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on Siemens Healthineers in accordance with this DPA, in particular such contract shall provide sufficient safeguards to implement appropriate technical and organizational measures in such a manner that the processing will meet 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. At the Customer's request, Siemens Healthineers shall provide a copy of such a sub-processor

agreement and any subsequent amendments to the Customer. To the extent necessary to protect business secrets or other confidential information, including personal data, Siemens Healthineers may redact the text of the agreement prior to sharing the copy.

6.2. A list of sub-processors is available at https://fleet.siemens-healthineers.com/welcome. Siemens Healthineers reserves the right to update this URL from time to time. Siemens Healthineers has the Customer's general authorization for the engagement of the listed companies as sub-processors.

The Customer shall subscribe to this Siemens Healthineers' website to receive the information regarding sub-processors and for any intended changes of that list through the addition or replacement of sub-processors. Siemens Healthineers is responsible for gathering the relevant information from sub-processors and keeping this list up to date.

The engagement or replacement of an additional sub-processor shall be deemed approved if Siemens Healthineers informs the Customer in advance thereof and the Customer raises no objection to Siemens Healthineers in writing, including in electronic form, within 30 days following such information.

6.3. If the Customer objects, the Customer shall notify Siemens Healthineers in detail about the reasons for the objection.

Following an objection, Siemens Healthineers may at its discretion

(i) propose another sub-processor in place of the rejected sub-processor; or

(ii) take steps to address the concerns raised by the Customer which remove the Customer's objection.

6.4. If the options as per Section 6.3 a. and b. are reasonably not available or the objection has not been removed otherwise, Siemens Healthineers 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 Healthineers to perform its contractual obligations.

6.5. 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 regarding Siemens Healthineers do not apply from the planned start date of the objected to sub-processor onwards. If Siemens Healthineers' performance obligations are terminated in part, the remuneration for the services unaffected by the partial termination shall be determined in accordance with Siemens Healthineers' standard list prices applicable to such services at Siemens Healthineers.

6.6. Where a sub-processor fails to meet its data protection obligations, Siemens Healthineers 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 Healthineers shall not be liable for damages and claims arising from the Customer's additional or alternate instructions as per Section 3.2 of this DPA.

6.7. In case a sub-processor in a third country (outside the EU/EEA) is engaged, data transfer mechanisms compliant with Articles 44 et seq. GDPR shall be used.

6.8. The Customer agrees that where a sub-processor is engaged in accordance with this Section 6 for carrying out specific processing activities (on behalf of the Customer) and those processing activities involve a transfer of personal data within the meaning of Articles 44 et seq. GDPR, compliance with Articles 44 et seq. GDPR can be ensured either by using standard data protection clauses adopted by the Commission in accordance with Article 46 (2) GDPR, provided the conditions for the use of those standard data protection clauses are met or by using other appropriate safeguards pursuant to Article 46 GDPR.

7. Assistance

7.1. Taking into account the nature of the processing as described in the main contract and this DPA, Siemens Healthineers 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.

7.2. Siemens Healthineers 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.

7.3. Taking into account the nature of the processing as described in the main contract and this DPA and the information available at Siemens Healthineers, Siemens Healthineers shall assist the Customer at the Customer's expense in ensuring Customer's own compliance with the obligations pursuant to

(i) Article 32 GDPR (security of processing);

(ii) Article 33 GDPR (notification of personal data breach to the supervisory authority);

In the event of a personal data breach concerning personal data processed by Siemens Healthineers, Siemens Healthineers shall notify the Customer without undue delay after Siemens Healthineers having become aware of the breach. Such notification shall contain, at least:

a. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b. the details of a contact point where more information concerning the personal data breach can be obtained;

c. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(iii) Article 34 GDPR (communication of a personal data breach to the data subject);

(iv) Article 35 GDPR (data protection impact assessment); and

(v) Article 36 GDPR (prior consultation).

7.4. If the Customer requires assistance, the Customer may contact the Office of the Siemens Healthineers Data Privacy Officer at dataprivacy.func@siemens-healthineers.com.

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 Healthineers 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. Until the data is deleted, Siemens Healthineers shall continue to ensure compliance with this DPA.

9. Information and Audit Rights

9.1. With regard to the processing under the main contract, Siemens Healthineers 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.

9.2. Siemens Healthineers 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 Healthineers 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 Healthineers. Prior to an Audit, the Parties shall mutually agree on the scope, timing, and duration of the audit. The Customer shall reimburse Siemens Healthineers for any services incurred by Siemens Healthineers with regard to the Audit at the then current Siemens Healthineers service rates, which shall be made available to the Customer upon request.

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

Attachment TOM:
Technical and Organizational Measures ("TOM") Siemens Healthineers

1. 1.Pseudonymization and Encryption of Personal Data

Siemens Healthineers 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 Healthineers encrypts personal data with symmetric or asymmetric keys.

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

2.1 Siemens Healthineers ensures confidentiality and integrity by taking the following measures:

Access control:

Siemens Healthineers 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 using a card reader system. Depending on the security category, property, buildings or individual areas are secured by additional measures. These 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 (at least 8 characters, regularly automatic expiration), employee ID cards with PKI encryption, password-protected screen savers in case of inactivity, intrusion detection systems and intrusion-prevention systems, regularly updated antivirus and spyware filters in the network and on the individual PCs 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 Healthineers 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.

2.2 Siemens Healthineers ensures systems and services constant availability and reliability by taking the following measures:

Siemens Healthineers 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 Healthineers shall restore the availability of and access to personal data in the event of a physical or technical incident by taking the following measures:

Siemens Healthineers stores personal data in RAID systems and integrates redundant systems according to security marking. Siemens Healthineers uses systems for uninterruptible power supplies (e. g. UPS, batteries, generators) to secure the power supply in the data centers.

Databases or data centers are mirrored in different physical locations.

A comprehensive written emergency plan is available. Emergency processes and systems are regularly reviewed.

4. Control Procedures to ensure the Safety of Processing

Siemens Healthineers maintains a control procedure 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 Healthineers 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.