Carestream GDPR Annex
Compliance with the EU General Data Protection Regulation

Recitals:

Carestream and the company to whom this GDPR Annex has been sent (the "Processor") have one or more written agreements (collectively, "the Agreements") pursuant to which the Processor provides services to Carestream (collectively, the "Services") that may entail the Processing of Personal Data (as defined below).

The European General Data Protection Regulation (GDPR) imposes specific obligation on Carestream and other companies (controllers) with regard to their vendor relationships. The GDPR requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

Each of the Agreements contains provisions requiring each party to comply with all applicable laws. This GDPR Annex documents the data protection requirements imposed upon the parties by the GDPR. This GDPR Annex is hereby incorporated by reference into each Agreement in order to demonstrate the parties' compliance with the GDPR.

1. For purposes of this Annex, "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation, together with any addition implementing legislation, rules or regulations that are issued by applicable supervisory authorities. Words and phrases in this Annex shall, to the greatest extent possible, have the meanings given to them in Article 4 of the GDPR. In particular:

   (a) "Personal Data" has the meaning to give it in Article 4(1) of the GDPR: "any information relating to an identified or identifiable natural person; 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," but only to the extent such personal data pertain residents of the European Economic Area (EEA) or are otherwise subject to the GDPR.

   (b) "Personal Data Breach" has the meaning given to it in Article 4(12) of the GDPR: "[any] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

   (c) "Processing" has the meaning given to it in Article 4(2) of the GDPR: "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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

   (d) "Subprocessor" means any processor as defined in Article 4(8) of the GDPR: "[any] natural or legal person, public authority, agency or other body which processes personal data" on behalf of the Processor (including any affiliate of the Processor).

   (e) "Transfer" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

2. In accordance with GDPR Article 28(1), Processor represents that it has implemented appropriate technical and organisational measures in such a manner that its Processing of Personal Data will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects.

3. In accordance with GDPR Article 28(2), the Processor shall not engage any Subprocessor without prior specific or general written authorisation of Carestream. In the case of general written authorisation, the Processor shall inform the

Carestream of any intended changes concerning the addition or replacement of other Subprocessors and give Carestream the opportunity to object to such changes. The Processor shall also comply with the requirements for subprocessing as set forth in Article 28(4), namely that the data protection obligations set forth herein (and as my otherwise be agreed by the Processor in the Agreements) such be imposed upon the Subprocessor, so that the Processor's contract with the Subprocessor contains sufficient guarantees that the Processing will meet the requirements of the GDPR.

4. In accordance with GDPR Article 28(3), the following terms are incorporated by reference into the Agreements:

   (a) The Processor shall only process the Personal Data only (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from Carestream, including with regard to any Transfers, and (iii) as needed to comply with law (in which case, the Processor shall provide prior notice to Carestream of such legal requirement, unless that law prohibits this disclosure);

   (b) Processor 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) Processor shall take all security measures required by GDPR Article 32, namely:
      i. 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, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

      ii. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

      iii. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process them except on instructions from Carestream, unless he or she is required to do so by EEA Member State law.

   (d) Taking into account the nature of the processing, Processor shall reasonably assist Carestream by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Carestream's obligation to respond to requests for exercising the data subject's rights;

   (e) Taking into account the nature of processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist Carestream to comply with) the obligations regarding Personal Data Breaches (as set forth in GDPR Articles 33 and 34), data protection impact assessments (as set forth in GDPR Article 35), and prior consultation (as set forth in GDPR Article 36);

   (f) At Carestream's discretion, the Processor shall delete or return all the Personal Data to Carestream after the end of the provision of services relating to Processing, and delete existing copies unless applicable EEA member state law requires storage of the Personal Data;

   (g) The Processor shall provide Carestream with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and allow for and contribute to audits, including inspections, conducted by Carestream or another auditor mandated by Carestream; and

(h) The Processor shall immediately inform Carestream if, in its opinion, an instruction infringes the GDPR other Union or Member State data protection provisions.

5. The Processor shall not Transfer any Personal Data (and shall not permit its Subprocessors to Transfer any Personal Data) without the prior consent of Carestream. The Processor understands that Carestream must approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as standard contractual clauses) unless another legal basis for the Transfer exists.

6. The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will notify Carestream without undue delay in the event of any Personal Data Breach.

7. The Processor shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Processor's activities for Carestream) Processor shall make them available to Carestream upon request.