Kodak Alaris
Data Processor Addendum & Standards

PARTIES

(1) Kodak Alaris Holdings Limited or one of its Affiliates **(Customer)**

(2) Supplier provides data processing services to Customer **(Provider)**

BACKGROUND

(A) The Customer and the Provider entered into an agreement under which Provider transfers, handles or otherwise holds data on behalf of Customer (**Master Agreement**) that may require the Provider to process Personal Data on behalf of the Customer. For the avoidance of doubt and for Customer's published standard terms and conditions and/or purchase orders (if any).

(B) Under the terms of the Master Agreement and Customer's Supplier Code of Conduct, Provider agreed to abide by all applicable privacy laws.

(C) This Data Processor Addendum & Standard (**Addensum**) sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services under the Master Agreement. This Addendum contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Addendum.

1.1 Definitions:

Authorised Persons: the persons or categories of persons that the Customer authorises to give the Provider personal data processing instructions as identified in *Annex A*.

Business Purposes: the services described in the Master Agreement or any other purpose specifically identified in *Annex A*.

Data Subject: an individual who is the subject of Personal Data.

Personal Data: means any information relating to an identified or identifiable natural person that is processed by the Provider as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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.

Processing, processes and process: either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes 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. Processing also includes transferring Personal Data to third parties.

Data Protection Legislation: all applicable privacy and data protection laws including the General Data Protection Regulation ((*EU) 2016/679*) and any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (*2002/58/EC*) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*).

Personal Data Breach: a 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.

Standard Contractual Clauses (SCC): the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, a completed copy of which comprises *Annex B*.

1.2 This Addendum is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this Addendum.

1.3 The Annexes form part of this Addendum and will have effect as if set out in full in the body of this Addendum. Any reference to this Addendum includes the Annexes.

1.4 A reference to writing or written includes faxes and/or email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Addendum and any provision contained in the Annexes, the provision in the body of this Addendum will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Addendum and any provision contained in the Annexes, the provision contained in the Annexes will prevail;

(c) any of the provisions of this Addendum and the provisions of the Master Agreement, the provisions of this Addendum will prevail; and

(d) any of the provisions of this Addendum and any executed SCC, the provisions of the executed SCC will prevail.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 The Customer and the Provider acknowledge that for the purpose of the Data Protection Legislation, the Customer is the controller and the Provider is the processor.

2.2 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Provider.

2.3 The Master Agreement describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Provider may process to fulfil the Business Purposes of the Master Agreement. Upon request, Provider shall provide Customer with its Record or Processor Activities which shall be substantially in the form of Annex A.

3. PROVIDER'S OBLIGATIONS

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Addendum or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Legislation.

3.2 The Provider must promptly comply with any Customer request or instruction requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Provider will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this Addendum specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Provider to process or disclose Personal Data, the Provider must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Provider will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.5 The Provider must promptly notify the Customer of any changes to Data Protection Legislation that may adversely affect the Provider's performance of the Master Agreement.

4. PROVIDER'S EMPLOYEES

4.1 The Provider will ensure that all employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Addendum.

5. SECURITY

5.1 The Provider must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data. Provider shall upon demand supply Customer its technical and organization measures which shall include security measures for the categories set out in *Annex C*.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including 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; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. PERSONAL DATA BREACH

6.1 The Provider will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Provider will restore such Personal Data at its own expense.

6.2 The Provider will without undue delay notify the Customer if it becomes aware of:

(a) any accidental, unauthorised or unlawful processing of the Personal Data; or

(b) any Personal Data Breach.

6.3 Where the Provider becomes aware of (a) and/or (b) above, it shall, without undue delay, also provide the Customer with the following information:

(a) description of the nature of (a) and/or (b), including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Provider will reasonably co-operate with the Customer in the Customer's handling of the matter, including:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.5 The Provider will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law.

6.6 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.7 The Provider will cover all reasonable expenses associated with the performance of the obligations under *Clause 6.2* and *Clause 6.4* unless the matter arose from the Customer's specific instructions, negligence, wilful default or breach of this Addendum, in which case the Customer will cover all reasonable expenses.

6.8 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to a Personal Data Breach to the extent that the Provider caused such a Personal Data Breach, including all costs of notice and any remedy as set out in *Clause 6.6*.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 The Provider (or any subcontractor) must not transfer or otherwise process Personal Data outside the European Economic Area (**EEA**) without obtaining the Customer's prior written consent.

7.2 Where such consent is granted, the Provider may only process, or permit the processing, of Personal Data outside the EEA under the following conditions:

(a) the Provider is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Provider must identify in *Annex A* the territory that is subject to such an adequacy finding; or

(b) the Provider participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Provider (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation (*(EU) 2016/679*). The Provider must identify in *Annex A* the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Provider must immediately inform the Customer of any change to that status; or

(c) the transfer otherwise complies with the Data Protection Legislation for the reasons set out in *Annex A*.

7.3 If any Personal Data transfer between the Customer and the Provider requires execution of SCC in order to comply with the Data Protection Legislation (where the Customer is the entity exporting Personal Data to the Provider outside the EEA), the parties will complete all relevant details in, and execute, the SCC contained in *Annex B*, and take all other actions required to legitimise the transfer.

8. SUBCONTRACTORS

8.1 The Provider may only authorise a third party (subcontractor) to process the Personal Data if:

(a) the Customer provides prior written consent prior to the appointment of each subcontractor **OR** is provided with an opportunity to object to the appointment of each subcontractor within three (3) days after the Provider supplies the Customer with full details regarding such subcontractor;

(b) the Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Addendum, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of such contracts;

(c) the Provider maintains control over all Personal Data it entrusts to the subcontractor; and

(d) the subcontractor's contract terminates automatically on termination of this Addendum for any reason.

8.2 Those subcontractors approved as at the commencement of this Addendum are as set out in *Annex A*. The Provider must list all approved subcontractors in Annex A and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

8.3 Where the subcontractor fails to fulfil its obligations under such written agreement, the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.5 The Parties consider the Provider to control any Personal Data controlled by or in the possession of its subcontractors.

8.6 On the Customer's written request, the Provider will audit a subcontractor's compliance with its obligations regarding the Customer's Personal Data and provide the Customer with the audit results.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD PARTY RIGHTS

9.1 The Provider must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

9.2 The Provider must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider must notify the Customer within five (5) working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 The Provider will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this Addendum or as required by law.

10. TERM AND TERMINATION

10.1 This Addendum will remain in full force and effect so long as:

(a) the Master Agreement remains in effect, or

(b) the Provider retains any Personal Data related to the Master Agreement in its possession or control (**Term**).

10.2 Any provision of this Addendum that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Data will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this Addendum is a material breach of the Master Agreement. In such event, the Customer may terminate effective immediately on written notice to the Provider without further liability or obligation.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation, they may terminate the Master Agreement on written notice to the other party.

11. DATA RETURN AND DESTRUCTION

11.1 At the Customer's request, the Provider will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Data related to this Addendum in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 The Provider will certify in writing that it has destroyed the Personal Data within five (5) days after it completes the destruction.

12. RECORDS

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Customer, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in *Clause 5.1* (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Addendum and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Annexes to this Addendum once a year.

13. AUDIT

13.1 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Addendum obligations during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

13.2 The notice requirements in *Clause 13.1* will not apply if the Customer reasonably believes that a Personal Data Breach occurred or is occurring, or the Provider is in breach of any of its obligations under this Addendum or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Addendum or any Data Protection Legislation, the Provider will:

(a) promptly conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within ten (10) days.

13.4 At the Customer's written request, the Provider will:

(a) conduct an information security audit before it first begins processing any Personal Data and repeat that audit on an annual basis;

(b) produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within ten (10) days.

13.5 At least once per year, the Provider will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Addendum, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

13.6 On the Customer's written request, the Provider will make all of the relevant audit reports available to the Customer for review.

13.7 The Provider will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Provider's management.

14. WARRANTIES

14.1 The Provider warrants and represents that:

(a) its employees, subcontractors, agents and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;

(b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(i)
the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

(ii)

the nature of the Personal Data protected; and

(iii)

comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in *Clause 5.1*.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

ANNEX A

Form Record of Processing Activities

(FOR DATA PROCESSORS)

This Record of Processing Activities (Record) describes how [COMPANY] [and its subsidiaries and affiliates in] [the United States/[COUNTRY]] [processes/process] personal data. [COMPANY] recognizes that Article 30 of the EU General Data Protection Regulation (GDPR) imposes documentation requirements on controllers and processors of data. This Record is company confidential information but [COMPANY] will provide it to the appropriate supervisory authority on request as required by Article 30.

Data Processor Details:

Name: [COMPANY NAME] (Data Processor)

Address: [COMPANY ADDRESS]

Telephone Number: [COMPANY TELEPHONE NUMBER]

Website: [COMPANY WEBSITE]

Data Controller: [COMPANY NAME AND CONTACT DETAILS]

[Representative: [NAME AND CONTACT DETAILS]]

[Data Protection Officer: [NAME AND CONTACT DETAILS]]

Categories of Processing

Data Processor processes personal data on behalf of [DATA CONTROLLER NAME] for the following purpose(s):

- [Research and analytics.
- Product development.
- Direct marketing.
- Professional and advisory services.
- IT system management.
- Information security.
- Human resources management.
- Payroll administration.
- Retirement plan administration.]

[Transfers of Personal Data to Third Countries or International Organizations

As part of **processing** personal data on behalf of [DATA CONTROLLER], Data Processor transfers personal data to the following [third countries] [and] [international organizations]:

- [[COUNTRY].]
- [[INTERNATIONAL ORGANIZATION].]]

[Data Processor makes limited personal data transfers subject to the second subparagraph of Article 49(1) which are necessary for [DATA CONTROLLER]'s compelling legitimate interests. Data processor provides appropriate safeguards for these limited personal data transfers through [contractual clauses/[OTHER MECHANISM]].]

Technical and Organizational Security Measures

Data Processor has implemented the following technical and organizational security measures to protect personal data:

- [Pseudonymisation of personal data.
- Encryption of personal data.

- Segregation of personal data from other networks.
- Access control and user authentication.
- Employee training on information security.
- Written information security policies and procedures.]

Changes to this Record of Processing Activities

[COMPANY] reserves the right to amend this Record of Processing Activities from time to time consistent with the GDPR and other applicable data protection requirements.

Effective Date:

[DATE]

Last modified:

[DATE]

ANNEX B
STANDARD CONTRACTUAL CLAUSES

The most recent clauses set forth at:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

shall be used.

ANNEX C
SECURITY MEASURES

Supplier to supply its technical and organizational data security measures such as:

- Physical access controls.
- System access controls.
- Data access controls.
- Transmission controls.
- Input controls.
- Data backups.
- Data segregation.