Kodak Requirements for AI Technology

These Kodak Requirements for AI Technology are mandatory for every Kodak Supplier that provides AI-enabled products, services, or apps to Kodak that include any "High Risk AI System" (as defined in the EU AI Act or other applicable Privacy Law) and to all AI Technology (including AI-powered features) intended to be integrated into Kodak's products or services. These Requirements allow Kodak and Supplier to demonstrate compliance with applicable AI and privacy laws. Capitalized terms used herein but not defined below have the meanings given to them in the Kodak Data Processing Agreement and/or the services agreement(s) between the parties.

1. **General Obligations.** Supplier represents: (a) to the extent it is the developer of the AI Technology, Supplier has implemented an appropriate AI Management Program; (b) to the extent that it is a licensor or deployer or a third party AI system, it is has conducted reasonable and appropriate due diligence on the AI system to confirm that it was developed pursuant to an appropriate AI Management Program. **"AI Management Program**" means written policies, procedures and instructions that reasonably designed to ensure (1) appropriate data governance of the AI Technology including for training and validation data, so that the inputs and outputs are properly permissioned, free of bias, and appropriate for the purposes for which they are provided, and (2) appropriate risk management, including identification and management of reasonably foreseeable risks, including the risk of algorithmic discrimination.

2. **High Risk AI Systems.** Supplier represents that any High Risk AI System meets all applicable legal requirements for such system, including (without limitation) those under the Privacy Laws. For illustration, Supplier shall (at minimum) implement appropriate risk management and data governance controls for such systems and shall at its own expense maintain all technical documentation and other records needed to demonstrate such compliance. Supplier shall provide this documentation to Kodak upon request and as required by law.

3. **AI Technology for Integration.**

3.1 Conformity. Supplier has provided specific information about the AI Technology to Kodak, and the parties have described the planned integration in the relevant Statement(s) of Work (SOW). Supplier agrees that the AI Technology will conform to Kodak's requirements (as given in the SOW) and to the documentation described below.

3.2 Documentation. Supplier shall maintain reasonable and appropriate technical and other documentation about its AI Technology and shall provide this documentation to Kodak upon request so that Kodak can understand the capabilities and limitations of the AI Technology and comply with its own obligations when integrating the AI Technology into its products and services. The documentation shall include:

(a) a general description of the AI Technology including hardware and software requirements, information on the architecture and number of parameters; modality (e.g. text, image); and information regarding any applicable licenses for the technology and any incorporated models,

(b) a description of the data elements, including format of the inputs,

(c) information on the data used for training, testing and validation, training time, and other relevant details related to the training,

(d) design specifications of the technology, including the general logic of the AI Technology, the systems, processes and algorithms, and the key design choices including the rationale and assumptions made,

(e) an assessment of the human oversight measures needed, including an assessment of the technical measures needed to facilitate the interpretation of the outputs of the AI Technology; and

(f) any other information required by the Privacy Laws.

Supplier shall keep the information available and up to date for the duration of provision of the relevant products and services. Kodak may, at any time upon reasonable request, audit the AI Technology against the technical documentation to confirm that the AI Technology complies with the applicable requirements and the Privacy Laws.

3.3 Intellectual Property. Supplier shall put in place a policy to comply with copyright and related intellectual property rights for the AI Technology.

3.4 Data governance. Data sets used by Supplier for training, validation and testing shall be subject to data governance practices appropriate for the purpose of the AI Technology. Supplier shall ensure that these data sets are relevant, sufficiently representative, and to the extent possible, free of errors and complete in view of the intended purpose. Data sets shall have the appropriate statistical properties, including, where applicable, with regard to the persons or groups of persons for whom the AI Technology is intended to be used.

3.5 Transparency.

(a) If the AI Technology is intended to interact directly with natural persons, it shall be designed so that the users are informed that they are interacting with an AI system or agent, unless this is obvious given the context of use.

(b) If the AI Technology generates synthetic audio, image, video or text content mark outputs in a machine-readable format, these outputs shall be detectable as artificially generated or manipulated in a way that is effective, interoperable, robust and reliable as far as technically feasible; this requirement is not applicable to the extent the AI Technology performs an assistive function for standard editing or do not substantially alter the input data provided by Kodak or the semantics thereof.

3.6 Explainability.

(a) Upon request, Supplier shall explain how the AI Technology arrived at a particular decision or outcome. At the minimum, this assistance will include a clear indication of the key factors that led the AI Technology to arrive at a particular result and the changes to the input that must be made in order for it to arrive at a different outcome.

(b) If the AI Technology is used to facilitate decisions that significantly affect persons or group of persons, Supplier shall provide Kodak with technical and other information required in order to explain how the AI Technology arrived at a particular decision or outcome and to offer the persons or group of persons on which the AI Technology is used the opportunity to verify the way in which the AI Technology arrived at that decision or outcome. Supplier grants Kodak the right to use, share and disclose this information, if and to the extent necessary to inform the persons or group of persons on which the AI Technology is used about the functioning of the AI Technology, or in any legal proceedings.

3.7 Resiliency and Security.

(a) Supplier's AI Management Program shall be designed to provide an appropriate level of accuracy, robustness, and cybersecurity for the AI Technology throughout their lifecycle.

(b) Supplier shall employ technical and organizational measures to help ensure that the AI Technology is resilient regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, including during its interaction with natural persons. Robustness may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

(c) If the AI Technology continues to learn during operations, it shall have controls implemented to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.

(d) The AI Technology shall be resilient against attempts by unauthorized third parties to alter its use, outputs or performance by exploiting system vulnerabilities. Technical solutions to ensure AI Technology's security shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause an AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.