Kodak Supplier Privacy & Security Terms

Supplier agrees that it shall comply with the following provisions with respect to all "Kodak Information" collected, used, transmitted or maintained for Eastman Kodak Company and its affiliates (collectively, "Kodak"). These Terms stipulate privacy, confidentiality, and security requirements and demonstrate compliance with applicable privacy, security and data protection laws.

1. Definitions.

(a) "Data Subject Request" means any request by an individual (or by another person acting on behalf of an individual) to exercise a right under any Privacy Law, or any other complaint or inquiry or similar communication about the Processing of the individual's Personal Information.

(b) "EEA Personal Data" means that subset of Personal Information consisting of personal data (as defined in GDPR) pertaining to residents of the European Economic Area (EEA), Switzerland and the United Kingdom.

(c) "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation.

(d) "Internal Control Report" means a Type II Service Organizational Control (SOC) report (based on the SSAE 16 or ISAE 3402 model) or any successor report thereto.

(e) "Kodak Information" means, collectively, all Personal Information and Sensitive Information Processed by Supplier for Kodak in connection with the Services.

(f) "Personal Information" means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, "personal data" (as defined in the GDPR) and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location.

(g) "Privacy Laws" means all applicable U.S. and international laws that regulate the Processing of Personal Information. In particular, "Privacy Laws the Privacy Laws may include (as applicable) the California Consumer Protection Act (CCPA), the GDPR, and other applicable laws that specify privacy, security or security breach notification obligations that affect the Personal Information or the provision of the services by Supplier.

(h) "Processing" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.

(i) "Security Breach" means a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law or any other event that compromises the security, confidentiality or integrity of Kodak Information.

(j) "Sensitive Information" means that subset of Personal Information and Kodak confidential business information, consisting of those data elements which, due to their nature has been classified by law or by Kodak policy as deserving additional privacy and security protections. Sensitive Information consists of: (i) all government-issued identification numbers, (ii) all financial account numbers (including payment card information) whether associated with a natural person or a legal person, (iii) individual medical records, genetic and biometric information, (iv) all data obtained from a U.S. consumer reporting agency (such as employee background investigation reports, credit reports, and credit scores), (v) user account credentials, such as usernames, passwords, security questions/answers and other password recovery data, and (v) data elements that constitute Special Categories of Data under the GDPR, namely EEA Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

(k) "Services" means any and all services that Kodak requests the Supplier to perform under the Agreement or any other contract or agreement that involves Processing of Kodak Information.

(l) "Subprocessor" means any third party (including an affiliate of Supplier) that provides any services to Supplier and that may have access (including inadvertent access) to any unencrypted Kodak Information.

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

2. <u>General Obligations</u>.

(a) Supplier shall only Process or Transfer Kodak Information as authorized by Kodak in writing and as necessary to perform the Services. Annex 1 contains a generally description of the Processing activities and Services, including contact information for those Supplier personnel who have primary responsibility for privacy and data security. Supplier may periodically update Annex 1 and provide the updated version to Kodak as needed to inform Kodak of any changes, including any changes to the privacy and security contacts, Subprocessors and/or Transfers.

(b) Supplier shall promptly inform Kodak in writing: (i) if it cannot comply with any material term of its agreement with Kodak regarding the Services (if this occurs, Supplier shall use reasonable efforts to remedy the non-compliance, and Kodak shall be entitled to terminate Supplier's further Processing of Kodak Information); (ii) of any request for access to any Kodak Information received from an individual who is (or claims to be) the subject of the data; (iii) of any request for access to any Kodak Information received by Supplier from any government official (including any data protection agency or law enforcement agency) unless it is explicitly prohibited by law

from notifying Kodak of the request; (iv) of any other requests with respect to Kodak Information received from Kodak's employees or other third parties, other than those set forth in the agreement. Supplier understands that it is not authorized to respond to these requests, unless explicitly authorized by Kodak or the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Supplier.

(c) Each party must use reasonable efforts to stay informed of the legal and regulatory requirements for its Processing of Kodak Information. Supplier's Processing shall comply with all Privacy Laws that are applicable to the Processing, as well as Supplier's own privacy notices. Supplier will promptly notify Kodak if, in its opinion, the instructions given by Kodak for Processing violate any law.

(d) Supplier has provided Kodak with responses to Kodak's Independent Service Provider Questionnaire (ISPQ) along with other information as needed to support those responses. Supplier represents and warrants that all such responses and information were accurate, current and complete, in all material respects.

(e) Once per year, Supplier shall provide Kodak with copies of applicable Internal Control Reports. Kodak understand that the responses and Internal Control Reports contain Confidential Information of the Supplier, and it shall not disclose the Internal Controls Reports other than to its auditors and advisors in connection with verifying Supplier's compliance with Kodak's security and privacy program requirements.

(f) Supplier shall reasonably cooperate with Kodak and with its affiliates and representatives in responding to Data Subject Requests and/or regulatory inquiries as needed for Kodak to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws. As may be required by Privacy Laws, Supplier will reasonably assist Kodak with any data protection impact assessments and prior consultations with regulators, in each case solely in relation to Processing of Kodak Data by Supplier.

3. **Specific Compliance Requirements.** To the extent applicable:

(a) Supplier certifies that it complies with those Privacy Laws that require such certifications, including (without limitation) the California Consumer Privacy Act (CCPA), and similar state statutes. With regard to Personal Information subject to CCPA and any similar laws, Supplier shall not (i) sell the Personal Information, (ii) retain, use or disclose the Personal Information other than as specified in the contract(s) with Kodak, as needed to perform the services and for appropriate Business Purposes (as defined in CCPA), (iii) retain, use or disclose the personal information outside of its direct business relationship with Kodak.

(b) If the Services involve the collection of Kodak Information directly from individuals, Supplier will provide the individuals with a clear and conspicuous privacy notice, which notice shall either (i) be Kodak's privacy notice, or (ii) be Supplier's privacy notice, provided that such notice must address any legal requirements for such notices in the jurisdictions where it is given, be translated into the languages used in connection with Supplier's interaction with the individuals, and indicate that Supplier is processing the data as a processor on behalf of its clients. All such notices must be approved by Kodak in writing.

(c) If the Kodak Information will include "protected health information" (or "PHI") as defined in the HIPAA Privacy and Security Rules, Supplier and Kodak shall execute an appropriate Business Associate Agreement as required by HIPAA.

(d) If the Kodak Information will include any payment card information, Supplier shall comply with all applicable requirements of the Payment Card Industry Data Security Standard as published by the PCI Security Standards Council (https://www.pcisecuritystandards.org/pci_security/).

(e) If the Kodak Information will include EEA Personal Data, Supplier and Kodak shall ensure adequate protection for the EEA Personal Data. Each party shall comply with the provisions of GDPR and other Privacy Laws applicable to it, as a "controller" or a "processor" (as defined in GDPR). For any Transfers of EEA Personal Data, the parties shall document adequate protection for the EEA Personal Data using an approved data transfer mechanism in accordance with section 5(b) below.

4. <u>Confidentiality and Data Access</u>.

(a) Consistent with the confidentiality provisions of the Agreement, Kodak Information is considered Confidential Information of Kodak and Supplier must maintain all Kodak Information in strict confidence. Supplier may disclose Kodak Information to its employees and contingent workers, but only to the extent such individuals require access to the Kodak Information to perform the Services.

(b) Prior to allowing any employee or contingent worker to Process any Kodak Information, Supplier shall (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement (in a form acceptable to Kodak), and (iii) provide the individual with appropriate privacy and security training. Supplier will also monitor its employees and contingent workers for compliance with the privacy and security program requirements.

5. <u>Approvals for Transfers and Subprocessors</u>.

(a) Supplier shall not Transfer the Kodak Information to any Subprocessors or other third parties unless such Processing is required to perform the Services and it has been explicitly authorized by Kodak in writing. Supplier shall provide Kodak with a list of all such Subprocessors within five (5) days of any request by Kodak for such list.

Notwithstanding the preceding paragraph, Kodak approves Transfers those Subprocessors listed on Annex 1 (as may be amended by the Supplier from time to time, as necessary to perform the Services), provided that the Supplier:

(i) Has conducted adequate due diligence on the Subprocessor to ensure that it is capable of providing the level of protection for Kodak Data as is required by these Terms;

(ii) Has entered into a written contract with the Subprocessor that includes terms equivalent to those contained in these Terms (offering the same level of protection for Kodak Data) and provides that the Subprocessor's right to Process Kodak Data can be terminated by Supplier immediately on expiry or termination of the Agreement for whatever reason; and

(iii) Remains primarily liable to Kodak for the acts, errors and omissions of the Subprocessor, as if they were Supplier's own acts, errors and omissions.

To the extent that these Transfers include any EEA Personal Data, Supplier shall indicate the cross-border transfer mechanism used to authorize the Transfer on Annex 1. Kodak reserves the right to object to any Subprocessor for good cause, and Supplier shall not allow Subprocessor to access Kodak Information until such objection is resolved.

(b) Supplier shall not Transfer the Kodak Information across any national borders or permit remote access to the Kodak Information from any Subprocessor or other third party outside of the country unless Supplier has the prior written consent of Kodak for such Transfer. Supplier understands that Kodak must authorize all such cross-border transfers, including by use of approved Transfer mechanisms. Notwithstanding the preceding, Kodak authorizes Supplier to make routine Transfers of Kodak Information in the normal course of business on its corporate systems to itself in other countries and to its affiliates, which are under common ownership with Vendor.

(c) Should EU authorities or courts determine that a Transfer mechanism selected by Supplier is no longer an appropriate basis for Transfers, Supplier and Kodak shall promptly take all steps reasonably necessary to demonstrate adequate protection for the EEA Personal Data, using another approved mechanism. Supplier understands and agrees that Kodak may terminate the Transfers as needed to comply with the EEA Privacy Laws.

6. <u>Information Security Requirements</u>.

(a) Supplier shall have implemented and documented appropriate administrative, technical and physical measures to protect Kodak Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. Supplier will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Supplier will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Kodak Information, and ensure that these risks are addressed.

(b) Supplier shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services (including restoring access to the Kodak Information) in a timely manner after a disruptive event. Supplier will regularly test and monitor the effectiveness of its business continuity and disaster recovered plans. At appropriate intervals or as otherwise requested by Kodak, Supplier will provide a copy of its written business continuity and disaster recovery plans to Kodak.

(c) If the Processing involves the transmission of Kodak Information over a network, Supplier shall have implemented appropriate supplementary measures to protect the Kodak Information against the specific risks presented by the Processing. Kodak Information may not be transmitted over any insecure network unless it has been appropriately encrypted.

(d) Kodak Information may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks, USB or flash drives, personal digital assistants (PDAs) or mobile phones, DVDs, CDs or computer tapes) unless it is encrypted.

(e) Upon request, Supplier shall provide Kodak with information about the Supplier's information security program. All such information is Confidential Information of Supplier. Supplier shall also submit its data processing facilities for audit, during Supplier's reasonable business hours, which shall be carried out by Kodak (or by a qualified independent auditor) in a mutually-agreeable manner (designed to validate Supplier's controls against an established industry standard such as ISO 27001) no more than ten (10) day after any such request. Supplier shall fully cooperate with any such audit. If any such audit reveals material gaps or weaknesses in Supplier's security program, Kodak shall be entitled to terminate Supplier's Processing of Kodak Information until such issues are resolved. Such audits may occur only once per year; provided however, that Kodak may audit at any time in the event of a security breach or suspected material violation by Supplier of its obligations under the Agreement. Supplier shall also cooperate with any audits conducted by any regulatory agency that has authority over Kodak as needed to comply with applicable law.

(f) Supplier will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Kodak Information. Supplier will notify Kodak within 24 hours upon discovery of any Security Breach. This notification must be made via email to WW-CISO-Mail@kodak.com. Supplier shall provide Kodak with all information about the Security Breach reasonably needed by Kodak to assess its incident response obligations.

If the Security Breach results from either (i) the negligence or misconduct of Supplier (or any Supplier Subprocessor) or (ii) a failure of Supplier to comply with the terms of this Standard or its Agreement with Kodak, Supplier shall bear all costs associated with resolving a Security Breach, including (without limitation), conducting an investigation, engaging appropriate forensic analysis, notifying individuals, regulators and others as required to by law or the Payment Card Industry Data Security Standard, providing individuals with credit monitoring (or other appropriate remediation service), and responding to individual, regulator and media inquiries. The costs associated by Supplier for investigating and mitigating any Incident (including providing notifications and credit monitoring as set forth above) shall not be limited by the caps on Supplier liability set forth in the Agreement (to the extent there are any). Supplier's other obligations with respect to liability and indemnification will be governed by the terms of the Agreement.

(g) When the Supplier ceases to perform Services for Kodak (and at any other time, upon request), Supplier will either (i) return the Kodak Information (and all media containing copies of the Kodak Information) to Kodak, or (ii) purge, delete and destroy the Kodak Information. Electronic media containing Kodak Information will be disposed of in a manner that renders the Kodak Information unrecoverable. Supplier will provide Kodak with an Officer's Certificate to certify its compliance with this provision. If Supplier is required by applicable law to retain any Kodak Information, Supplier warrants that it shall (i) ensure the continued confidentiality and security of the Kodak Information, (ii) securely delete or destroy the Kodak Information when the legal retention period has expired, and (iii) not actively Process the Kodak Information other than as needed for to comply with law.

(h) Supplier shall maintain appropriate cyber liability insurance to address the risks from its Processing of the Kodak Information, which shall include coverage for, but not limited to, network security liability and liability under Privacy Laws including risks of cyber-attacks and security breaches. Kodak shall be named as an additional insured under such Cyber Liability insurance.

* * *

Annex 1 – General Description of the Processing Activities

Additional Annexes (only if needed)

Annex 2 - EU Model Contract
(The attached must be completed only if Supplier will be Processing (as defined) EEA Personal Data)
[Attached, please see 2 Appendices – complete if needed, otherwise delete]

Annex 3 - HIPAA Business Associate Agreement
[Before providing medical or health insurance data of any US employee to Supplier, contact Benefits Director (HR Organization)]

Annex 1: General Description of Processing

Supplier Privacy and Security Contacts:
Primary Privacy or Data Protection Contact:_____
Primary Security Contact:_____
Data Protection Officer(s) *if applicable*:_____

Categories of PI: *(Please describe the Kodak Data that will be Processed under the Agreement.)* _____

_____

The Kodak Data include:

☐ EEA Personal Data ☐ Protected Health Information (subject to the US HIPAA Rules)
Personal Information about residents of: ☐ California ☐ Argentina, ☐ Brazil, ☐ Canada, ☐ Israel

Categories of Sensitive Information: *Please indicate if the Kodak Data will include any Sensitive Personal Information.*

☐ Government-issued identification numbers
☐ Online account access information, including usernames, passwords
☐ Financial account numbers, including payment card data
☐ Health data, health insurance data, genetic information and biometric information
☐ Consumer reporting data, including employment background screening reports
☐ Data related to criminal convictions or offenses or allegations of crimes
☐ Online or device identifiers, advertising identifiers, data used for online targeting
☐ Special categories of data that reveal race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life or sexual orientation

Categories of Data Subjects: *(Indicate the types of individuals whose data are being processed):*

☐ Consumers, website visitors
☐ Job applicants
☐ Prospective customers
☐ Suppliers
☐ Employees, contractors, dependents/family
☐ Kodak commercial customers
☐ Professionals, trade show attendees,
☐ Other _____

Description of Services: *(Brief overview of the Services and the purposes for which the Personal Information will be processed.* _____

_____

Physical Location(s) of the Personal Information: *(Where processing is carried out and where the Kodak Data are stored.)* _____

Data Transfers: *Please indicate how transfers of EEA Personal Data (if any) are authorized.*

_____ There are no Transfers of EEA Personal Data.

_____ Supplier has certified its compliance to the EU-US and Swiss-EU Privacy Shield Program (and has indicated in its filing that UK personal data remain covered by the certification). Supplier will maintain its certifications to the Privacy Shield for so long as it maintains any EEA Personal Data.

_____ Supplier will enter into approved EU Standard Contractual Clauses (Processors), a copy of which is incorporated into the Agreement as Annex 2. For purposes of the Standard Contractual Clauses, Kodak (or the applicable Kodak affiliate, or a corporate customer) will act as the "data exporter" and Supplier (or its approved Subprocessor, as applicable) will act as the "data importer."

_____ Supplier will Transfer EEA Personal Data pursuant to its approved set of Binding Corporate Rules for Data Processors.

_____ Supplier represents and warrants that all Transfers of EEA Personal Information to the Subprocessors listed on Annex 1 below are authorized using an approved mechanism.

Retention of Kodak Personal Information: *Please indicate how long the Kodak Data will be retained by Supplier and its Subprocessors (if any).*

☐ Kodak Data will be deleted automatically upon termination of the Agreement

☐ Kodak Data will be deleted upon termination of the Agreement if requested by Kodak

☐ Kodak Data will be retained after termination: *please describe the data retention rules and controls that exist to prevent further Processing of the Kodak Data by the Supplier and the Subprocessors (if any).* _____

_____

Annex 1 - Approved Subprocessors

Subprocessor Name	Subprocessor Address	Description of the Services Provided	Categories of PI	Location of the Processing (list all)	Transfer Mechanism (if EEA Data)

Annex 2
Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: .....
Address: .....
Tel. .....; fax .....; e-mail: .....
Other information needed to identify the organization
.....
(the data exporter)

And

Name of the data importing organization: .....
Address: .....
Tel. .....; fax .....; e-mail: .....
Other information needed to identify the organization:
.....
(the data importer)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 - Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; EN L 39/10

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer[1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorized access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses. EN 12.2.2010 Official Journal of the European Union L 39/13

Clause 7 - Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 - Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses[2]. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

[Signature Page follows]

[2] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter:
Name (written out in full): .....
Position: .....
Address: .....
Other information necessary in order for the contract to be binding (if any): (stamp of organization)

Signature .....

On behalf of the data importer:
Name (written out in full): .....
Position: .....
Address: .....
Other information necessary in order for the contract to be binding (if any): (stamp of organization)

Signature .....

Appendix 1
Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix 1.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
.....
.....
.....

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
.....
.....
.....

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
.....
.....
.....

Categories of data
The personal data transferred concern the following categories of data (please specify):
.....
.....
.....

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
.....
.....
.....

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
.....
.....
.....

DATA EXPORTER
Name: .....
Authorized Signature .....

DATA IMPORTER
Name: .....
Authorized Signature .....

Appendix 2
Standard Contractual Clauses

This Appendix 2 forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):
.....
.....
.....
.....