

## DATA PROCESSING AGREEMENT

### SECTION 1: TERMS

**1. BACKGROUND AND OBJECTIVE.** Within the scope of the Agreement, Supplier will gain access to and process Personal Data for which Customer is the Data Controller. This means that Supplier is a Data Processor in accordance with the applicable Data Protection Legislation. The objective of this DPA is to comply with the requirements in the Data Protection Legislation for a written agreement between the Supplier and the Customer.

**2. DEFINITIONS.** Unless otherwise defined, the terms used in this DPA shall have the same meaning as in the Data Protection Legislation:

**‘Data Controller’** means anyone who alone or jointly with others determines the purposes and means of the Processing of Personal Data;

**‘Data Protection Legislation’** means all the laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to:

- a) European Union member states: the General Data Protection Regulation (EU) 2016/679 (**‘GDPR’**) and any applicable national legislation implementing the GDPR.
- b) UK: Data Protection Act 2018.
- c) Argentina: the Argentinian Privacy Principles, as defined in Argentine Personal Data Protection Law 25 326.
- d) Australia: Australian Privacy Principles, as defined in the Australian Privacy Act 1988 (Cth).
- e) Brazil: **‘LGPD’** or the Brazilian General Data Protection Regulation, Law N° 13.709/2018.
- f) California: California Consumer Privacy Act (CCPA).
- g) Canada: Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
- h) Chile: Chilean Law 19,628 on the Protection of Private Life.
- i) Colombia: Colombian Law 1581 of 2012 and Decree 1074 of 2015.
- j) Mexico: Mexican Federal Law on the Protection of Personal Data held by Private Parties.
- k) Japan: Japanese Act on Protection of Personal Information and relevant guidelines issued by the Personal Information Protection Commission of Japan.
- l) South Korea: Korean Personal Data Protection Law and Law on Information and Communications Network Utilization and Information Protection.

**‘Data Processor’** means anyone who processes Personal Data on behalf of the Data Controller;

**‘DPA’** means this Data Processing Agreement;

**‘Personal Data’** means any information that, directly or indirectly, can identify a living natural person, as defined by the Data Protection Legislation;

**‘Processing’**, **‘Process’** means any operation or set of operations performed with regard to Personal Data, whether or not performed by automated means, for example collection, recording, organisation, storage, adaptation or alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction;

**‘Sub-Processor’** means a sub-contractor that is engaged by the Supplier. The Sub-Processor processes Personal Data on behalf of the Customer in accordance with the Sub-Processor’s obligation to provide its services to the Supplier.

**3. UNDERTAKING AND INSTRUCTION.** The Supplier undertakes to Process the Personal Data that it has access to under the Agreement on behalf of the Customer, for the purpose of fulfilling the Agreement. The Supplier further undertakes to:

- (a) Process the Personal Data in accordance with the Agreement and any other documented instructions from the Customer. The Supplier may, however, without instructions Process information required by any applicable laws, but shall inform the Customer of such requirement prior to Processing, provided that the Supplier is not prohibited to give such information in accordance with such applicable laws;
- (b) ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) implement all appropriate technical, physical, administrative and organisational measures necessary in order to ensure a level of security appropriate to the risk, as required pursuant to the Data Protection Legislation;
- (d) assist the Customer, taking into account the nature of the Processing, by implementing appropriate technical, physical, administrative and organisational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to and to fulfil requests from data subjects exercising their rights laid down in the Data Protection Legislation;
- (e) assist the Customer in ensuring compliance with the obligations in the Data Protection Legislation relating to implementing security measures, managing Personal Data breaches, conducting data privacy impact assessments and participating in prior consultations with the supervisory authority, at all times taking into account the nature of the Processing and the information available to the Supplier; and
- (f) promptly notify to the Customer any Personal Data breach (security incident), in order for the Customer to be able to comply with its obligations under the Data Protection Legislation to notify the supervisory authority and/or the data subjects in some cases.

The Supplier shall at the Customer's request, provide any other information reasonably requested by the Customer to assist the Customer in complying with the relevant Data Protection Legislation and/or inquiries from the supervisory authority.

**4. AUDIT.** The Supplier shall grant the Customer access to reasonable information necessary to demonstrate that the obligations set out in this DPA are complied with. The Customer shall give at least sixty (60) calendar days written notice to the Supplier prior to any audit. Audits shall be organised during Supplier's normal working hours. The Supplier shall facilitate and participate in audits, including inspections, carried out by the Customer or a governmental authority or by a third party authorised by the Customer. If the Customer uses a third party to carry out the audit, that third party shall not be a competitor of the Supplier and shall undertake confidentiality in relation to the Supplier's business information. The Supplier shall promptly inform and consult with the Customer in the event that a supervisory authority initiates or takes any action in relation to the Supplier with regard to the Processing of Personal Data under the Agreement or this DPA.

**5. ENGAGING SUB-PROCESSORS.** The Customer gives the Supplier a general authorisation to engage as Sub-Processors, to support the fulfilment of the Agreement: any other entities from time to time who are under common ownership and control of Supplier's parent company, Elekta AB ('**Affiliates**').

The Customer grants Supplier and Affiliates a general authorization to appoint the following types of Sub-Processors to support the fulfilment of the Agreement: Supplier and its Affiliates' cloud, software engineering, and other firms providing information technology and security advisory and support services; third party data center operators, and providers of outsourced technical support services.

The Sub-Processors engaged at the time of entering into the DPA are listed in Section 2. However, the Supplier shall inform the Customer of any plans regarding the engagement of new Sub-Processors, or replacement of Sub-Processors, so that the Customer is given an opportunity to object to such changes.

In the event that the Supplier engages a Sub-Processor for the Processing of Personal Data on the Customer's behalf, the Supplier and the Sub-Processor shall enter into a written data Processing agreement that imposes equivalent obligations on the Sub-Processor as those specified in this DPA. In the event that the Supplier engages a Sub-Processor outside of the country where the Customer is based, legal grounds for the transfer to a third country shall be secured, for example by entering into an appropriate data transfer agreement. The Supplier is hereby given the mandate and mission to enter into a data transfer agreement on the Customer's account in such case. The Supplier is liable, in all respects, for the Sub-Processor as for itself.

**6. OBLIGATION TO DELETE PERSONAL DATA.** Personal Data shall not be stored for a longer period than it is necessary to carry out the original purpose for the Processing. Where an application permits the Customer to migrate Personal Data held by the application and the Customer agrees to migrate any and all Personal Data prior to termination of the Agreement, the Supplier shall use reasonable commercial endeavours to permit the Customer to use the migrate function until expiry of the Agreement. Where the Agreement is terminated with immediate effect due to the Customer's breach, the Supplier shall use reasonable commercial endeavours to permit the Customer to use the migrate function in the period of 10 days after such termination.

For applications where no migration functionality is available for the Customer to independently use, the Customer and Supplier shall collaborate to transfer any and all Personal Data to the Customer for archival purposes upon the expiry or termination of the Agreement.

The Supplier is not obligated to store any of the Customer's Personal Data after expiry of the Agreement. The Supplier shall no later than 30 days after expiry of the Agreement effectively delete all Personal Data. For the purposes of this provision to effectively delete shall mean that the data is deleted in accordance with best practice industry standards so that Personal Data cannot be reconstructed using any known technology.

Without limiting the aforementioned, at any given time during the term of this DPA the Supplier shall effectively delete Personal Data to the extent requested by the Customer.

The obligation to delete Personal Data does not apply if storage of Personal Data is required pursuant to Data Protection Legislation, needed in order to fulfil Supplier's obligations under the Agreement or if Supplier is required by other applicable laws to retain the data.

**7. DAMAGES.** The Supplier's total liability for its performance under this DPA shall not exceed the price paid by the Customer under the Agreement in the twelve (12) months immediately preceding the claim that gave rise to the liability. For the avoidance of doubt, administrative fines are imposed on the Party in breach of its obligations and, in consequence, neither Party will bear the other Party's administrative fines.

**8. COMPENSATION.** The Parties agree that the Supplier's remuneration under the Agreement does not include compensation for the Supplier's measures and activities required to fulfil the DPA. The Supplier shall be entitled to compensation on a time and material basis for any work and documented costs for measures and activities taken in order to fulfil its undertakings under the DPA.

**9. BREACH.** In the event that the Supplier is in breach of its obligations under the DPA, the Supplier must remedy the breach within thirty (30) days of being notified of the breach, or within the time period agreed between the Parties.



**10. TERM.** The DPA is effective from the commencement the Agreement and for as long as the Supplier Processes Personal Data on the Customer's behalf. When the Agreement expires or terminates, the Supplier shall, based on the Customer's instructions, delete or return to the Customer, in a manner acceptable to the Customer, all Personal Data, and delete existing copies unless storage of Personal Data is required pursuant to any applicable laws or otherwise permitted in accordance with this DPA.

**11. CONFLICTS.** This DPA constitutes the entire agreement and understanding of the Parties and supersedes any previous agreement between the Parties relating to the subject matter of this DPA. Notwithstanding the foregoing, for US Customers, the terms and conditions in this DPA apply in addition to those in the Business Associate Agreement, and in the event of a conflict between this DPA and the Business Associate Agreement, the terms and conditions of this DPA shall prevail.

## **SECTION 2: INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA**

The Processing of Customer Personal Data by the Supplier may vary depending on the Products, Software applications and/or Services purchased from or licensed by the Supplier as follows:

### **1. THE PURPOSES OF THE PROCESSING**

The Supplier will Process the Personal Data of the Customer to the extent it is necessary in order to fulfil the Agreement with the Customer, to improve and further develop its Products and Services (i.e. for evaluating usability), or as otherwise agreed between the Customer and the Supplier in writing.

Further, in relation to Elekta Axis and Elekta Cloud-based software:

#### **a) For Kaiku Health:**

Supplier provides Customer with a cloud-based service for digital patient monitoring and management used by patients and staff of the Customer. Patient users can report on their health and wellbeing using predefined metrics (patient-reported data) such as symptoms or Quality of Life, receive reminders, notifications and instructions related to reporting the predefined metrics, and access patient materials that are provided by hospital or relevant third parties. Healthcare professional users can assign patients to predefined and individualized Patient Monitoring and Management Modules; receive, input and view patient metrics (e.g. quality of life metrics and symptoms); and view dashboards on individual patients and patient populations of predefined metrics.

#### **b) For MOSAIQ® Oncology Analytics (on Elekta Axis):**

Supplier provides MOSAIQ Oncology Analytics, a cloud based solution hosted by Supplier using Microsoft Azure platform. To guide and support the Customer in setting up/configuring custom reports by extracting data (including personal data) from Customer's MOSAIQ system(s) and other systems, Supplier may also Process Personal Data. The purpose for the Customer is to

optimize clinical operations and identify trends, inefficiencies, resource utilizations, analyze outcomes, and potential cost savings.

#### **c) For MOSAIQ SmartClinic (on Elekta Axis):**

MOSAIQ SmartClinic provides mobile access to a set of MOSAIQ functions and a Patient Synopsis. For the MOSAIQ SmartClinic on Elekta Cloud, Supplier provides Customer with a cloud based solution hosted by Supplier using Microsoft Azure platform. In addition to mobility, it also contains 'Smart' features which provide easier visualization, navigation, automation and notification of activities that need processes to manage patient care.

#### **d) For ProKnow (on Elekta Axis):**

Supplier provides Customer with a cloud-based RT-PACS (Radiation Therapy Picture/Patient Archiving and Communication System), hosted by Supplier using the Microsoft Azure platform. ProKnow is capable of archiving patient data, managing treatment planning information, and performing large cohort analysis with a focus on the data and images specific to radiation oncology patients.

In relation to order fulfillment and remote Services:

#### **e) For Order Fulfillment and on-site Services:**

Supplier may be onsite at Customer's facility to perform order fulfillment services, including but not limited to, site planning, installation, de-installation of Elekta Products and/or on-site provision of maintenance and support Services. Customer will take reasonable actions to protect the confidentiality and privacy of Personal Data. In the event Supplier is exposed to any Personal Data, the terms and conditions of this DPA will apply.

#### **f) For IntelliMax:**

Supplier provides Customer with remote access via Elekta IntelliMax with the capability to transfer files to provide technical support and predictive maintenance of Elekta products. No personal health information (PHI) or Personal Data is actively processed (accessed, viewed, stored, etc.) by Supplier unless Customer displays it on the end product during the session or transfers it to Supplier. In the event Supplier is exposed to any Personal Data, the terms and conditions of this DPA will apply.

### **2. CATEGORIES OF PROCESSING ACTIVITIES**

The Processing activities may include:

- a) Storing/hosting of Personal Data in proprietary reporting database (Elekta Axis on Microsoft Azure).

- b) Local and remote support for assistance and maintenance on radiosurgery and oncology radiotherapy equipment provided by the Supplier.
- c) Managing and responding to Customer service requests. This can include:
  - Escalation of service requests;
  - Troubleshooting and remote service for equipment;
  - Managing offsite repair, refurbishment or disposal of equipment or defective components
- d) Providing technical support for the relevant products;
- e) Developing and implementing customized imaging protocols for the Customer;
- f) Providing additional or advanced services to which the Customer has subscribed;
- g) Systems integration, data migration and installation operations (CT, PACS, etc.)
- h) Extraction, Transformation and Load (ETL) of personal data from relevant systems.
- i) Customer data can include access to application, audit logging information, use of application features etc.
- j) Facilitating reports to Customers.
- k) Analysis of the patient data in order to provide analytics to the Customer as described in the Agreement.
- l) Export/transfer of personal data from cloud based solution for the purpose of offline review or archival. This is usually done by the Customer.
- m) Compute, networking, and storage within a cloud environment.
- n) Product and service improvement, enhancement and development.
- o) Providing remote service support and IT-facility management (monitoring and supporting platform and applications and maintaining equipment);
- p) Providing software engineering, software maintenance, systems maintenance, including managing the availability, latency, scalability and efficiency of the Services;
- q) Anonymising the Processed Personal Data to provide the Service as per the Service description (i.e. for training artificial intelligence models) and for improving and further developing the service (i.e. for evaluating usability). For Kaiku Health, the Supplier may use the anonymised data in further developing the Service and transfer anonymous data to third parties (e.g.

its partners such as life sciences companies) for use in research and development and post-market surveillance. Supplier is responsible for ensuring the anonymity of the anonymised data. Description of the anonymisation techniques applied is available upon request.

### 3. CATEGORIES OF DATA SUBJECTS

- ✓ Customer employees
- ✓ Supplier employees or Supplier's Sub-Processor employees
- ✓ Customer patient data

### 4. CATEGORIES OF PERSONAL DATA

- a) Concerning Customer's employees and Supplier employees, the Supplier may Process Personal Data and contact information (e.g. e-mail, phone number etc.), as well as name and location of the institution in which an examination was conducted and name of the Customer employees performing an examination or log files and entries made into the Services by the Customer/Supplier's employee.
- b) Concerning Customer's patients, the Supplier may Process:
  - Information provided to the Service by the data subject (such as forms and messages);
  - Data provided to the Service by the employees of the Customer, concerning the care, monitoring, or planning of the care of the data subject;
  - Data obtained by Customer from other databases, concerning the care, monitoring, or planning of the care of the data subject;
  - Personal Data and contact information (i.e. e-mail, phone number, address, Next of Kin, Emergency Contact, Ethnicity, Religious);
  - Social information (Marital status; Tobacco, Alcohol, Drug Use, etc.);
  - Personal Data relating to patient health. This may include:
    - o Patient health status and diagnosis data;
    - o Parameter / settings of the equipment , and in particular : weight, height, temperature, age (in years or date of birth), gender , heart rate, image acquisition protocol, radiation dose, number of images, examination results;

- Parameters and description of protocols and examination procedures;
- Exam / serial / image numbers or other examination values generated by a system and assigned by the equipment for each exam;
- Images of the anatomy of a patient;
- Treatment Information including: Diagnosis; Labs; Vitals, Assessments; Transactional Document info; Orders; Appointments; Quality Check List; Charges; Provider Names, Provider IDs, Provider contact information.

Patient data may include Protected Health Information (PHI) as defined under US legislation and any other activities related to patient care. Under the EU GDPR, this data may fall under the definition of special category of personal data.

## 5. SUB-PROCESSORS AND PLACES WHERE THE SUB-PROCESSING IS CARRIED OUT

The following Sub-Processors may currently be engaged by the Supplier and the Customer approves of Supplier's engagement of these sub-processors to provide the Processing activities:

Elekta AB and its Affiliates from time to time, including without limitation:

- Elekta Limited, UK
- Elekta Inc, USA
- Elekta B.V., Netherlands
- Elekta Instrument AB, Sweden

Dependent on Customer location, additional Elekta Affiliates may provide local support (e.g. language support, license software maintenance and support, application development, testing, and support, and providing Customer outreach and support).

Microsoft

Parametric Technology UK Ltd

Salesforce

Servicemax

Dell Boomi

Hytec

## 6. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

The Supplier shall perform its obligations and actions under this DPA with all due skill, care and diligence.

The Supplier shall use technical and organizational security measures appropriate to prevent the harm which might result from any unauthorized or unlawful processing, loss, destruction, damage, alternation to or disclosure of the Personal Data and having regard to the nature of the Personal Data which is to be protected.

Customer acknowledges and agrees that the nature of the Services mean that the technical and organizational measures may be updated by Supplier from time to time but such updates shall not result in a lesser standard of security to that in place at the time of signing this DPA

Should the Supplier become aware of any non-conformity with the security requirements set out above, either within its own or within the subcontractor's organization, such non-conformity shall be notified to the Customer in accordance with the Personal Data Breach procedure set out in this DPA.



EXHIBIT MTERMS AND CONDITIONS FOR MOSAIQ ONCOLOGY ANALYTICS ('MOA') The terms and conditions contained in this Exhibit shall apply to all MOSAIQ ONCOLOGY ANALYTICS. 1

. DEFINITIONS. 1.1 'Named Users' shall mean current employee or agent of the Customer that has been issued a User ID by the Customer allowing such individual to access and use MOA as authorized in this Agreement. 2 'Customer Data' means the Customer data input that is transmitted to and maintained at the Cloud Service by Supplier in compliance with this Agreement for incorporation into the Customer Database. 1.3 'Customer Database(s)' means the Customer Data stored in the MOA databases that are specific to the Customer. 1.4 'Cloud Service' means the remote facility where the MOA and Customer Databases are installed and maintained for information processing, transmission and data storage services for the MOA. Supplier shall provide access to the remote system through a secure global computer communications network ('Internet'). 1.5 'ISP' shall mean Internet Service Provider, a third party providing Customer with high speed access to the internet. 1.6 'Separate Terms' refers to separate license terms, specified in the Scope of Supply or provided separately, that apply to Separately Licensed Third Party Technology. 1.7 'Separately Licensed Third Party Technology' refers to third party technology that is licensed under Separate Terms and not under the terms of this Agreement. 2. GRANT OF LICENSE. Subject to the provisions of this Agreement, the Supplier hereby grants to the Customer, and the Customer hereby accepts from the Supplier, a nonexclusive, nontransferable, non-assignable limited license to use the MOA utilizing Supplier's Cloud Services for internal purposes only during the term specified in Section 6. The Customer acknowledges and agrees that



the MOA is the proprietary information and a trade secret of the Supplier and its Affiliates and that this Agreement grants the Customer no title or rights of ownership in the MOA. The Customer agrees not to market, sublicense, make derivative works of, distribute, permit timeshare, or allow any other access to the MOA other than for the Customer's own internal use as permitted hereby.

Customer Databases and Customer patient data stored in the MOA Cloud are and shall remain the exclusive property of the Customer. The Customer also understands and agrees that for the MOA listed in Exhibit A, Scope of Supply, licensed to Customer for use with the Cloud Service provided hereunder, (i) the provisions of this Section 2 of this Exhibit shall apply, and (ii) the Customer is only authorized to use MOA through the Cloud Service pursuant to this Agreement. 3.

ACCEPTANCE. Customer shall inspect MOA promptly upon receipt of delivery. Unless Customer objects in writing within five (5) business days after first use, completion of on-site training, installation or receipt of packing slip from Elekta, whichever occurs first, Customer shall be deemed to have accepted MOA as of the date of such first use, completion of on-site training, installation or receipt of packing slip from Elekta ('Acceptance'). 4. AUTHORIZED USE. Customer

is authorized to use MOA only as a cloud based solution (per the Specification) at the Site and in compliance with all applicable local, state, national and foreign laws, treaties and regulations, including those related to data privacy, international communications, export laws and the transmission of technical or personal data laws.

Customer is not authorized to: (a) copy or duplicate, or permit anyone else to copy or duplicate, any physical, magnetic, or other version of the MOA; (b) create or attempt to create, reverse engineer or otherwise, the source

modify the MOA in any manner. 5. MOA WARRANTY. Each party represents and warrants that it has the legal power and authority to enter into this Agreement. Supplier warrants that, (i) at the time MOA is delivered to Customer and throughout the term of this Agreement, it will be free of material defects in materials and workmanship, and (ii) the Cloud Services will comply with the applicable documentation in all material respects. Customer's exclusive remedy, and Suppliers sole liability, with respect to any breach of this Section 5 will be for Supplier to use commercially reasonable efforts to promptly correct the applicable defects (provided that Customer notifies Supplier in writing of such defect within the applicable warranty period). If Supplier is unable, after reasonable effort, to cause MOA to perform substantially in accordance with its Specifications, then this Agreement may be terminated with respect to MOA at the option of either party hereto without further obligation or liability. In the event this Agreement is terminated during the initial one (1) year limited warranty period for MOA, Supplier shall refund to Customer all license fees paid by Customer for MOA. Supplier shall have no liability for misuse or modification of MOA by Customer. Supplier's entire liability, and Customer's exclusive remedy, during the Warranty Period will be, at Supplier's option, to attempt to correct or work around errors or to refund the License Fee for the affected the MOA. Any refund is subject to Customer ceasing use of MOA. Notwithstanding the foregoing, Supplier's warranty does not cover: (a) defects arising out of unauthorized repair, alteration or modification; (b) defects emanating from improper application, improper installation or operation on equipment other than Designated Equipment; or (c) accidental damage, negligence in use, improper storage, electrical power damage, or



abnormal operating conditions. This section provides the exclusive remedies for all claims based on failure of or defect in the MOA and this warranty is exclusive and are in lieu of all other warranties, conditions, and guarantees whether written, oral, implied, or statutory. EXCEPT FOR

THE EXPRESS LIMITED WARRANTIES PROVIDED IN THIS SECTION, SUPPLIER MAKES NO EXPRESS WARRANTIES FOR MOA. SUPPLIER SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES FOR MOA INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE TO THE EXTENT PERMITTED BY APPLICABLE LAWS. WITHOUT LIMITING THE FOREGOING, SUPPLIER DOES NOT WARRANT THAT THE OPERATION OF MOA WILL BE

UNINTERRUPTED OR ERROR FREE. Any remedial steps taken by Supplier hereunder shall not extend the applicable warranty period. Any unauthorized modification of MOA by Customer or any failure by Customer to implement any improvements or updates to MOA as supplied by Supplier or its representative shall void any and all of Supplier's obligations with respect to MOA. 6.

TERM & TERMINATION. The license granted under this Section 6 shall commence upon Acceptance, as defined within this Agreement, of MOA by Customer and shall continue for the license term specified on the cover page hereof unless sooner terminated in accordance with the provisions of this Agreement. Supplier shall have the right to terminate any license granted or discontinue delivery of any cloud based delivery immediately upon written notice to Customer without further obligation or liability to Customer if:

(a) Customer commits any breach of this Agreement; (b) any sublicense, assignment or transfer or attempted sublicense, assignment or

transfer by Customer of MOA is made without the written consent of Supplier; (c) any transport, movement or attempted transport or movement by customer of MOA, or the Designated Equipment on which the MOA is operated on, from the Site is made; (d) any modification or adaptation of MOA is made or any attempt to use MOA with any products other than the Hardware is made; or (e) any use of MOA in connection with or on other equipment than the Designated Equipment. 7. CONSEQUENCES OF TERMINATION. Upon the termination of the license to MOA, Customer shall immediately: (a) return modifications of MOA and all copies of any documentation, notes, and other materials with respect to MOA; (b) purge all copies of MOA or any portion thereof from all Designated Equipment and from any computer storage device or medium on which Customer has placed or has permitted others to place MOA; and (c) deliver to Supplier a written certification that Customer has complied with all of its obligations under this section. 8. LIMITATIONS ON SUPPLIER'S OBLIGATIONS. Customer understands and agrees that Supplier may develop and market new or different computer programs which use part or all of MOA and which perform all or part of the functions performed by MOA. Nothing contained in this Agreement gives Customer any rights with respect to such new or different computer programs. 9. SUPPORT SERVICES. Subject to the terms, conditions and fees set forth in this Exhibit, Supplier will provide Customer with the support services specified in this Section for MOA. Supplier will provide such assistance as is necessary to cause MOA to perform substantially in accordance with its Specifications by providing a suitable 'fix,' 'patch,' or 'work around' for the problem or a statement that an appropriate 'fix' will be included in a future release of MOA, the time period within which the

release is expected to be issued and a commitment to provide the release at no cost to Customer. New MOA licenses are not included in Supplier's support services and will be offered by Supplier to Customer at Supplier's then current published prices and on such other terms and conditions as are acceptable to Supplier. 10. THIRD PARTY TECHNOLOGY. MOA may contain or require the use of Separately Licensed Third Party Technology. If applicable, Customer is responsible for complying with the Separate Terms specified by Supplier that govern the use of Separately Licensed Third Party Technology. The third party owner or provider of such Separately Licensed Third Party Technology retains all ownership and intellectual property rights in and to such Separately Licensed Third Party Technology. Additionally, Separately Licensed Third Party Technology shall be subject to the terms set forth in Section 14 of the Standard Terms for Sale. 11. SUPPLIER RESPONSIBILITIES 11.1 The Supplier, pursuant to the terms of this Agreement and these MOA Terms, shall be responsible for: a) Within commercially reasonable constraints, provide a secure and redundant environment to operate the applicable MOA Cloud Service. b) Selecting equipment for the Cloud Service appropriate to the configuration requirements of MOA and which are compatible with the existing

Cloud architecture to deliver MOA Cloud Service.

c) The installation and/or configuration of MOA Cloud Services in accordance with this Agreement

d) With participation by the Customer, configuration of MOA. e) Periodic monitoring of the utilization and performance of MOA Cloud Service. f) Ensure that backups of the Customer Databases are maintained at all times.

1. The Supplier's Recovery Time Objective when the database is completely down, which is the time it takes to restore a corrupt database, is approximately 4 hours. g) Provide real-time anti-virus monitoring using updated virus definition on MOA installed in the Cloud. h) Notify Customer at least 90 days in advance, if possible, of any planned changes to MOA Cloud. 11.2

Notwithstanding the foregoing, Supplier shall not be responsible for: a) The performance or use by Customer of any services by any third party communications services provider or damages caused based on such use or inability to use such services. b) Transmission or communication errors or other problems with transmission of Customer Data by Customer to the Cloud Service.

12. CUSTOMER RESPONSIBILITIES In order to ensure that Supplier is able to deliver the Cloud Service and meet the performance standards set forth in these MOA Terms, Customer shall be responsible for, in addition to other provisions in this Agreement: a) Designate primary and secondary liaisons that have been trained on the applicable MOA and Cloud Service methods to provide Supplier with all necessary after-hours contact information for such individuals. b) Installation and maintenance of all hardware for MOA at Customer facilities required to use the Cloud Service. c) Notify the Supplier in writing of any planned Customer-side configuration changes that could affect the Suppliers ability to deliver Cloud Service or impact the performance of the Cloud