GENERAL TERMS AND CONDITIONS

The General Terms and Conditions herewith shall form a part and parcel of the Service Agreement.

1. DEFINITIONS:

1.1 ***"Applicable Laws"*** mean and include all applicable laws of Thailand including all rules, regulations, notifications, guidelines, governmental orders and bye-laws as in force from time to time that may be required to be complied by Service Provider herein.

1.2 ***"Confidential Information"*** shall mean any non-public information including but not limited to personally identifiable information, protected health information, intellectual property, products, system techniques, data, software, know how, improvements, developments, techniques, documents, designs, methods, processes, programs, presentations, business plans, marketing plans, strategic information, pricing lists, and business information, customer information, architecture, pattern, compilation, algorithm, forecasts, licenses, financial affairs, personnel matters, operating procedures, organization responsibilities, formula, flow chart, marketing matters, policies or procedures, confidential information of third parties, scientific, technical, commercial, the Service Agreement and any other information that Service Provider may come to know of or may come to possess including information which is disclosed prior to the execution of the Service Agreement by Receiver to Service Provider, whether orally or in written form and includes information which by its nature is confidential.

1.3 **"Controller", "Processor"** 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;

1.4 "**Data Protection Laws**" – all laws, rules, regulations, and orders of any jurisdiction or subdivision thereof relating to the privacy, security, confidentiality and/or integrity of Personal Data that are applicable to the operations, services or products of Service Provider and the Receiver.

1.5 "**Data Security Breach**" – (a) the loss, inadvertent disclosure, unauthorized access to or acquisition of or misuse of Personal Data or any media containing Personal Data; (b) the disclosure or use of Personal Data in a manner inconsistent with Data Protection Laws or the Service Agreement; or (c) any other act or omission that negatively impacts the security, confidentiality, and/or integrity of Personal Data.

1.6 "**Data Subject**" mean an identified or identifiable person whose Personal Data are processed, accessed, received, transmitted, deleted, or maintained by the Service Provider on behalf of and under the instruction of the Receiver. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

1.7 ***"Deliverables"*** mean and include all documents, goods or other similar items, correspondence, plans, video or audio media, computer programs or software for Receiver or other similar items created by Service Provider, exclusively for Receiver and/or required to be delivered under the Service Agreement or any relevant SOW.

1.8 **"Good Industry Practice"** means, the exercise of reasonable skill and care, implementation of industry standards, efficiency, security, promptness, timeliness, diligence, in a professional manner, as expected from a skilled, trained and experienced professional provider of similar services, including but not limited to Security Industry Practice;

1.9 ***"Intellectual Property Rights"*** means all copyrights, know-how, Confidential Information and rights to create derivative works and all rights in registered or unregistered patents, trademarks, trade

secrets, designs or inventions, proprietary right or form of intellectual property (whether protectable by registration or not), customer list, Service Agreement, specification, formula, device, drawing programme, system, process, logo, mark or style, business, Receiver, domain or product names and mark works including without limitation any other intellectual property rights in Thailand.

1.10 **"Parties"** means collectively the Receiver and Service Provider;

1.11 "**Personal Data**" – any information that relates to an identified or identifiable person including without limitation electronic data and paper based files that is Processed directly or indirectly, by Service Provider or Service Provider Subcontractors on behalf of and as instructed by the Receiver. This may include: name or initials, home or other physical address, cell/mobile or telephone number; photograph and/or any data or information subject to Data Protection Laws. Personal Data includes Special/Sensitive Personal Data as defined below.

1.12 "**Process, Processed, Processing**" – any handling of Personal Data by any means, including, without limitation, collecting, accessing, receiving, using, transferring, retrieving, manipulating, recording, organizing, storing, maintaining, hosting, adapting, altering, possessing, sharing, disclosing (by transmission, dissemination or otherwise making available), blocking, erasing, destroying, selling, or licensing.

1.13 **"Security Industry Practice"** means, then-current and applicable practices as defined in the International Organization for Standardization (ISO/IEC) ISO/IEC ISO27001, ISO/IEC 27002:2013, SSAE-16, ISAE3402, National Institute of Standards and Technology (NIST) NIST 800-44, the Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications, and the Center for Internet Security (CIS) Standards (or any successor to these security standards) or any other industry security standards mutually agreed by Parties;

1.14 **"Security Incident"** means an actual or imminent event which may impact the Receiver Data confidentiality, integrity, availability or resilience;

1.15 ***"Services"*** mean and include Services including deliverables as described in the Service Agreement entered between the parties in the format as may be prescribed by Receiver from time to time and accepted by Service Provider.

1.16 "**Service Provider**" means the performer and provider of the Services under the Service Agreement as described in the Service Agreement.

1.17 "**Service Provider Subcontractor**" means any third party that assists Service Provider in performing its obligations under the Service Agreement, including an affiliate or direct or indirect subcontractor of Service Provider.

1.18 "**Special/Sensitive Personal Data**" means, including, without limitation, (i) an individual's physical, physiological or mental characteristics, economic status, racial or ethnic origin, political, ideological, religious opinions or philosophical beliefs, trade union membership, health or medical information including information related to payment for health services, sex life or sexual preference, genetic material or information, medical records and history, human biological samples or cells, biometric information, personality profiles or (ii) an individual's name or initials in combination with the individual's (1) adhaar number, (2) driver's license number, (3) passport number, visa number or other government identifier, (4) credit card, debit card, or other financial account numbers, with or without any associated code or password that would permit access to such account, or (5) mother's maiden name. Special/Sensitive Personal Data is a subset of Personal Data.

1.19 **"The Receiver Data"** means all data, documents or records of whatever nature (including Personal Data and the Receiver's Confidential Information) and in whatever form relating to the business of the Receiver including details of customers, employees or otherwise, whether subsisting

before or after the date of the Service Agreement and whether created or processed as part of, or in connection with, the Services or provided by the Receiver (or third parties acting on their behalf) to Service Provider in connection with the Service Agreement;

1.20 "The Receiver's Environment" means any the Receiver's system, the Receiver's data center, 3rd party system owned by or licensed to the Receiver, infrastructure managed by the Receiver, the Receiver's Affiliate or the Receiver's sub-contractor or any other system, interface or infrastructure as notified by the Receiver from time to time;

1.21 "Third Party Code" means the Alcon Third Party Code as referenced in the Service Agreement;

1.22 "The Data Exporter" means the controller who transfers the personal data;

1.23 "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;

1.24 "The Subprocessor" means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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;

1.25 "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;

1.26 "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.

1.27 *"Term"* means the period from when the Service Agreement shall become effective i.e. on the Effective Date and until the End Date (both days inclusive) as specified in the Service Agreement, unless earlier terminated in accordance with Section 4 (Termination) of this General Terms and Conditions. Parties agree that the Term shall not exceed beyond the period of 3 years from the Effective Date.

Part-1
Commercial Terms

2. SERVICES:

2.1 Service Provider agrees to provide Services to Receiver and Receiver agrees to receive such Services from Service Provider on the terms and conditions contained in the Service Agreement and in this General Terms and Conditions.

2.2 Service Provider shall provide Services in a timely, diligent, professional manner and in accordance with best industry practices and applicable laws. Service Provider agrees to perform Services at the indicated service levels through appropriately qualified resources as more particularly specified in the Service Agreement or as agreed between the parties in writing from time to time. Service Provider shall supervise the performance of Services. Time is the essence of this engagement.

2.3 Service Provider shall promptly inform Receiver in writing about any unforeseen results, problems, difficulties deficiencies etc. with regard to Services.

2.4 Upon written request of Service Provider, Receiver shall provide to Service Provider such information including Confidential Information and data as Receiver determines to be required by Service Provider for the due performance of Services.

2.5 Receiver has engaged Service Provider to render Services on a non-exclusive basis i.e. Receiver shall be entitled to approach or engage any other third party for rendering the same or similar services at any point in time.

2.6 Receiver reserves the right to cancel, amend, vary, and modify any Services or part thereof any time under intimation to Service Provider. No such cancellation, amendment, variation or modification shall affect Service Provider's right to be paid for Services actually rendered. The Service Provider agrees to refund to Receiver the consideration paid to Service Provider, if any, that are no longer required to be provided by Service Provider.

2.7 If any services, other than those retained by Receiver under the Service Agreement, are reasonably required for, and incidental to or inherent in, the proper performance and provision of Services (regardless of whether they are specifically described in the Service Agreement), they shall be deemed to be implied by and included within the scope of Services to be provided by Service Provider to the same extent and in the same manner as if specifically described in the Service Agreement.

3. FEES & EXPENSES:

3.1 In consideration of the services, agreed to be performed by Service Provider, Receiver agrees to pay to Service Provider, a fee for the Services, as set out in the Service Agreement.

3.2 Service Provider shall send an invoice to Receiver to the attention of such person and at such address as may be designated by Receiver from time to time.

3.3 Unless otherwise, Service Provider will invoice monthly in arrears for delivered Services during the previous month. Service Provider must provide appropriate supporting documentation to substantiate the amount charged, if request by Receiver.

3.4 Permissible reimbursable expenses, if any, shall be reimbursed to the Service Provider, together with the fees for the services. The invoice sent to Receiver by Service Provider shall include the fee payable for Services and the permitted reimbursable expenses separately. Receipts or other evidence of payment of the permitted expenses must be sent to Receiver together with the corresponding invoice.

3.5 All undisputed payments shall be made by Receiver within a period of sixty (60) days or within such other time period as specified in the Service Agreement, subject to the satisfactory completion of associated services or supply of deliverables, from the date of receipt of an approved invoice.

3.6 The fees payable under this agreement are subject to withholding tax as required under the applicable law. Service Provider shall be liable for all transaction taxes on the services rendered under the Agreement.

4. TERMINATION:

4.1 The Service Agreement may be terminated by Receiver for convenience, at any time, by providing thirty (30) days prior written notice to Service Provider.

4.2 Either party shall have the right to terminate the Service Agreement immediately at any time by written notice to the other party, if such party:

(a) is in breach of any of its obligations under the Agreement and fails or is unable to remedy such breach within a period of thirty (30) days of receipt of notice in writing specifying such breach.

(b) is or states that it is unable to pay its debts as they fall due, enters into any scheme of arrangement or composition with, or assignment for the benefit of all or any class or creditors, is wound up or has a liquidator, provisional liquidator, receiver and manager or statutory or other official manager appointed over all or any part of its property.

4.3 Notwithstanding anything contained herein, Receiver alone shall be entitled to terminate the Agreement immediately in the event of Service Provider committing a breach of Section 6 (Confidentiality, Data Protection and Data Management), Section 9 (Obligations, Representations, Warranties and undertaking), Section 11 (Compliance with Law and Alcon Guidelines), Section 12 (Alcon Anti Bribery Guidelines) and/or Section 16 (Audit) of this General Terms and Conditions or has undergone a change in control which adversely affects the performance of the Agreement; or has a conflict of interest which adversely affects the performance of this agreement.

4.4 Upon the expiry or termination of the Service Agreement, the Service Provider shall discontinue Services in the most cost effective manner and without any costs to Receiver.

4.5 If the Agreement is terminated in terms of Section 4.2 (a) and/or 4.3 (Termination) as above attributable to the breach by Service Provider; in that event, Receiver shall have no further obligations under the Service Agreement. Specifically Receiver shall not be liable to pay any fees or costs incurred by Service Provider under this Service Agreement except any outstanding fee for service rendered.

4.6 Termination of the Service Agreement shall be without prejudice to any claim or right of action of either party against the other party for any breach of the Service Agreement. The provisions of Section 5 (Indemnification), Section 6 (Confidentiality, Data Protection and Data Management), Section 8 (Intellectual Property) and Section 9 (Obligations, Representations, Warranties and Undertakings) of this General Terms and Conditions shall survive the termination or expiration of the Service Agreement.

5. INDEMNIFICATION:

5.1 Parties agrees to indemnify, defend and hold the other Party (including all its officers, directors, employees, contractors and agents) harmless from and against any and all third party claims, demands, causes of action, damages, liabilities, losses, costs and expenses, including attorneys' fees (collectively, the "**Claims**"), arising out of, to, or resulting directly or indirectly from the action or omission of the Party (including but not limited to Party's employees representatives, officers or sub-contractors), and/or due to breach by the Party of any of its warranties, representations, covenants and obligations under the Agreement and/or due to any third party infringement claims with respect to any Intellectual Property Rights.

Part-2

Governance

6. CONFIDENTIALITY, DATA PROTECTION AND DATA MANAGEMENT:

6.1 Parties agrees and undertakes to treat all Confidential Information as confidential, except for information which Parties are able to demonstrate, through appropriate documentation, that is:

a. in the possession of Party at the time it was received from the other Party;
b. generally available to the public;
c. developed by either Party, independent from and without reliance on Confidential Information.

6.2 Nothing in this Section 6 shall prevent the disclosure of those parts of Confidential Information which is required to be disclosed by law or court order; provided however that, if Party is so required to disclose any Confidential Information, it shall provide the other Party with a prompt written notice

of such requirement, so that other Party may seek a protective order or other appropriate remedy to prevent or limit such disclosure.

6.3 Service Provider agrees and undertakes that Confidential Information shall be used only during the term and exclusively for the purposes of the Service Agreement and shall not be disclosed to any third party. Employees of the parties and their affiliates and permitted consultants or sub-contractors are bound by confidentiality obligations not less strict than those set out herein. Such aforementioned personnel will not be regarded as third parties.

6.4 After the expiry or early termination, howsoever caused, of the Service Agreement, Service Provider shall return to Receiver or at Receiver's option destroy and not make copies of any documents supplied by Receiver to Service Provider under the Agreement.

6.5 Service Provider agrees that it will be responsible and liable for breach of this Section 6 by any of its employees, agents, contractors and consultants.

6.6 The obligations set forth in this Section 6 shall also be applicable to information received by either Party while negotiating the Service Agreement and the obligation under this Section 6 shall remain in effect during Term of the Service Agreement and for a period of five (5) years following the expiration or early termination of the Service Agreement.

7. PERSONAL DATA PRIVACY AND PROTECTION

7.1 The Service Provider shall comply with the Section 7.3 on **Data Protection Requirements** and the Section 7.4 on **Additional Information Security Requirements** as specified below, in case the service includes collection, processing and handling of Data not arising out of Europe Union.

7.2 The Service Provider shall comply with the Section 7.4 on **Additional Information Security Requirements** as specified below and the terms in Exhibit 3 of this General Terms and Conditions, in case the service includes collection, processing and handling of European Union Data.

7.3 Data protection requirements:

7.3.1 Technical and Organizational Measures

a. The Service Provider shall carry out Processing activities on Personal Data solely for the purpose specified in the Service Agreement and as instructed by the Receiver. All persons who have access to Personal Data must maintain its confidentiality, the limitation of use to specific purposes, and access shall be permitted on a need-to-know basis to the extent required for the performance of Service Provider's obligations. Service Provider shall ensure that all persons who have access to Personal Data have received appropriate privacy and security training, which shall be updated periodically in accordance with applicable laws, regulations, and industry standards, or as otherwise requested by the Receiver. Service Provider shall not use or disclose any Personal Data that Service Provider creates, receives, maintains, or transmits as a result of performance of the Service Provider's obligations, other than as expressly permitted or required by the Service Agreement.

b. The Service Provider shall establish the minimum technical security and organizational measures referenced in the Alcon Third Party Code together with any additional requirements, if applicable, set forth under Additional Information Security Requirements. The technical and organisational measures are subject to technical advancements and development. In this regard, it is permissible for Service Provider to implement alternative adequate measures so long as the minimum defined level of security is not reduced. Substantial changes must be documented.

c. Throughout the term of the Service Agreement, Service Provider will maintain and monitor a comprehensive, written privacy and information security program, including data protection policies and procedures, and consistent with any privacy compliance plan established between the parties and attached hereto, that contains administrative, technical and physical safeguards designed to protect against reasonably anticipated threats to the security, confidentiality or integrity of, and the unauthorized Processing of, Personal Data. Service Provider will periodically assess reasonably

foreseeable risks to the security, confidentiality, integrity, and resilience of electronic, paper and other records containing Personal Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks.

7.3.2 Rectification, restriction and erasure of Personal Data

a. The Service Provider may not on its own authority rectify, erase or restrict the processing of Personal Data that is being processed on behalf of the Receiver, except by written instructions from the Receiver. Service Provider will notify the Receiver promptly (and in any event within five business days from receipt) of any communication received from a Data Subject relating to the Data Subject's rights to access, modify or correct Personal Data and to comply with all instructions of the Receiver in responding to such communications

d. Insofar as it is part of the scope of the Service Agreement, the right to erasure, 'right to be forgotten', rectification, data portability and access shall be ensured by the Service Provider in accordance with documented instructions from the Receiver without undue delay.

7.3.3 Quality assurance and other duties of Service Provider

a. Service Provider shall provide the Receiver with the contact details of Service Provider's data protection officer (where appointment is required by local law) for the purposes of direct contact. The Receiver shall be informed within twenty-four (24) hours of any change of the data protection officer.

b. Service Provider will notify the Receiver in writing and as soon as practical of any request made by any government, law enforcement or regulatory agency (but no later than one (1) business day from the date of any such request) for information concerning, or access to, Personal Data, unless notification to the Receiver is prohibited by Data Protection Laws or other applicable laws, rules, regulations or orders. Service Provider will cooperate with the Receiver in responding to such requests.

c. The Receiver shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to the Processing of Personal Data. This also applies insofar as the Service Provider is under investigation or is party to an investigation by a competent authority in connection with infringements to any civil or criminal law, or administrative rule or regulation regarding the processing of Personal Data in connection with the Agreement.

7.3.4 Service Provider Subcontracting

a. Subcontracting for the purpose of this Data Protection Requirement are to be understood as meaning services which relate directly to the provision of the principal obligation related to the processing of Personal Data pursuant to the Service Agreement. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment.

b. Service Provider understands and agrees that, without limitation, the confidentiality, privacy and security requirements contained in the Service Agreement and this General Terms and Conditions also apply to any permitted Service Provider Subcontractors, temporary employees or other third-parties who receive any Personal Data as a result of the Service Agreement. Service Provider shall only enter into sub-contract agreements that include data protection provisions no less restrictive than the provisions set forth in this Data Protection Requirement. Upon written request by the Receiver, copies of such sub-contracts shall be provided to the Receiver within seven (7) business days. The Receiver must be granted (a) the right to monitor and inspect Service Provider Subcontractors upon reasonable notice and (b) the right to obtain information from Service Provider about the substance of the sub-contract and the implementation of the data protection obligations within the sub-contract relationship, upon written request.

7.3.5 Data Security Breach

a. At any time during the processing of Personal Data, Service Provider shall notify the Receiver immediately of any Data Security Breach involving Personal Data, including any breach at facilities, systems or equipment of Service Provider's subcontractors. Service Provider agrees to assist and cooperate with the Receiver concerning any disclosures to affected parties, government or regulatory agencies and with any other remedial measures requested by the Receiver or required under any law. Service Provider will take such mutually agreeable steps to prevent the continuation or repetition of such Data Security Breach.

b. Unless otherwise required by applicable Data Protection Laws or any other law, rule, regulation or order, Service Provider will make no disclosures to affected parties or any government, law enforcement or regulatory agencies concerning a Data Security Breach relating to the Personal Data except as directed by the Receiver. Notwithstanding the foregoing, Service Provider may contact local police in the event of a physical breach of Service Provider facilities or theft of equipment or documents.

c. Service Provider will assist and cooperate with the Receiver concerning any disclosures to such parties or agencies, and with any other remedial measures requested by the Receiver or required under any law, rule, regulation or order applicable to Service Provider or the Receiver, at Service Provider's expense, including providing notice to Data Subjects of a Data Security Breach and providing credit monitoring services to such individuals.

7.3.6 Deletion and return of Personal Data

a. Copies or duplicates of Personal Data shall never be created without the knowledge of the Receiver, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as Personal Data required to meet regulatory requirements to retain data.

b. Upon termination or expiration of the Service Agreement, or as requested in writing by the Receiver at any time, Service Provider will, at its own expense and at the Receiver's option: (a) promptly return all Personal Data; or (b) destroy all documents, materials, and any other media that may contain Personal Data, without retaining any portion or copy thereof. Service Provider will provide the Receiver with a Certificate of Destruction of Personal Data in a form acceptable to the Receiver, signed by an authorized employee of Service Provider who has supervised such destruction.

7.4 Additional Information Security Requirements:

These Additional Information Security Requirements ("**AISRs**") are intended to supplement any other information security requirements that may be contained in the terms and conditions of the Service Agreement, including without limitation the Minimum Information Security Requirements referenced in the Alcon Third Party Code (such other information security requirements being referred to as "**Baseline Requirements**"). In the case of a conflict between the Baseline Requirements and the AISRs, the stricter requirement (from an information security perspective) shall prevail. The Service Provider agrees and acknowledges that the AISRs form part of the Service Agreement.

In these AISRs the following capitalized expressions shall have the following meanings unless stated otherwise or the context requires otherwise:

7.4.1 Service Provider Assessments:

a. The Receiver or nominated third party has the right to monitor, inspect and assess organizational, technical and administrative safeguards maintained by Service Provider and any respective measures employed to ensure security, availability, integrity and resilience of the Receiver Data including without limitation processes, policies, systems, business continuity test report and infrastructure. Service Provider shall provide records and evidence about such measures in form and

timescale reasonably requested by the Receiver. Service Provider shall cooperate and support the Receiver or nominated third party in such assessment. Without prejudice to the aforementioned rights of the Receiver, Service Provider shall (or shall procure that its hosting provider shall) maintain third party certifications or audit reports as stipulated by the Receiver either under the Service Agreement or by a separate written communication.

b. The Receiver shall have the right to perform detailed technical on-site or off-site assessments evaluating effectiveness of implemented measures to ensure confidentiality, availability, integrity and resilience of the platform. Report(s) from such assessment will be provided to Service Provider and Service Provider shall remediate gaps as defined in Section 7.4.1.e of the Additional Information Security Requirements.

c. Service Provider shall ensure penetration and security tests are periodically performed in alignment with Good Industry Practice covering then-current known vulnerabilities on the environment where the Receiver Data is being processed to identify gaps that help increase security.

d. No more than once per calendar year (if not triggered by gaps identified during previous penetration testing, independent assessments or another previous the Receiver assessment) the Receiver may perform or contract to perform, at its own expense, an application and infrastructure penetration test. Report(s) from penetration tests will be provided to Service Provider and Service Provider shall remediate gaps as defined in Section 7.4.1.e of the Additional Information Security Requirements..

e. Service Provider shall remediate any identified gaps without undue delay but not later than as defined in the remediation plan. The Parties agree that a second occurrence of assessment result in material non-compliance or Service Provider's failure to remediate deficiencies according to the remediation plan shall be deemed as an irremediable material breach of the Service Agreement.

7.4.2 Services to be provided according recognized standards:

a. Service Provider shall process, treat and handle the Receiver Data in accordance with Good Industry Practice.

7.4.3 Minimum encryption and continuity standards:

a. Service Provider shall utilize at least 256-bit AES (symmetric) or 4096-bit (asymmetric) RSA encryption or equivalent state of the art cryptographic techniques approved by the Receiver and TLS 1.2 at minimum

7.4.4 The Receiver Environment:

a. Service Provider acknowledges and accepts that any interface, connection or interaction with the Receiver Environment shall be done only after documented approval from the Receiver (which may already be included as part of the Service Agreement). Such connection to the Receiver Environment shall be maintained, protected and tested in line with Security Industry Practice as mutually agreed between the Parties and connection may be terminated or requested to be terminated by the Receiver at any time at its sole discretion.

b. Service Provider shall ensure that no: (a) viruses or other harmful code intended to disable, damage or provide unauthorized access; or (b) code used to keylogging or any software used to enforce licensing restrictions; or (c) any other code providing functionality not intentionally accepted by the Receiver in writing is infiltrated into the Receiver Environment by Service Provider or it personnel (including without limitation, in all of the three aforementioned cases as a result of failure

to observe the requirements as defined in Section 7.4.1.e of the Additional Information Security Requirements.

c. Service Provider shall extract and access only data as defined by the Receiver and shall inform immediately the Receiver if Service Provider is able to access or extract other data than specified by the Receiver. Such notification should follow the provisions on Security Incident notification as defined in Clause 8.

7.4.5 Service Provider personnel with access to the Receiver Environment:

a. In the event that any Service Provider personnel: (i) receives a Receiver issued badge (or other access mechanism) providing them with access to the Receiver premises; (ii) a personalized the Receiver network access account (e.g. a Receiver 5-2-1 account) the Receiver laptop, or (iii) a the Receiver e-mail account, or (iv) other type of access to the Receiver Environment, Service Provider shall ensure that such Service Provider personnel shall follow any applicable information security policies of the Receiver and participate in the Receiver trainings at no costs to the Receiver. Service Provider shall notify the Receiver without undue delay of any changes to the status of Service Provider's or Service Provider subcontractor's personnel that may affect the right to access to the Receiver Environment. Such status changes may include without limitation termination of personnel's employment relationship, change in area of work/responsibilities or termination of subcontractor's engagement.

7.4.6 Return of the Receiver Data:

a. As an alternative option to the disposal of the Receiver Data, the Receiver shall have the right to receive such the Receiver Data in the form and timescale specified by the Receiver.

7.4.7 Security Incidents:

a. Service Provider shall monitor, analyze and respond to Security Incidents as defined in this Clause 8. Service Provider will engage and report to the Receiver if there is any actual or suspected Security Incident which could impact the Receiver or the Receiver Data. Confirmed Security Incident is always considered as priority 1 incident.

b. The Receiver contact for reporting Security Incident identified by Service Provider: privacy@alcon.com

c. Service Provider shall follow as a minimum the following Security Incident management process:

1) Service Provider shall notify the Receiver without undue delay, but not later than twenty four (24) hours after Security Incident was evidenced.
2) If Security Incident is confirmed, Service Provider shall take appropriate actions to minimize further exposure of the Receiver Data in consultation with the Receiver without undue delay, but not later than in forty eight (48) hours after Security Incident was confirmed, where such actions shall include without limitation:
    - stopping inappropriate access or any other inappropriate activities with the Receiver Data;
    - defining remediation actions to prevent repetition of such Security Incident;
    - restoring normal operations of the Services; and
    - informing the Receiver periodically on progress of remediation actions.

After above actions preventing repetition of Security Incident are implemented, Service Provider shall provide a written report to the Receiver detailing actions performed and safeguards implemented.

7.4.8 Patch management:

a. Service Provider shall monitor available patches, evaluate, test and implement them in a timely manner for any systems involved in support of the Services or in the processing of the Receiver Data.

b. If a patch has been evaluated to not be applied, Service Provider shall ensure: a) alternative controls or safeguards are implemented to ensure the confidentiality, integrity and availability for any systems involved in support of the Services or in the processing of the Receiver Data; or b) evidence indicating the evaluation, the risk it potentially imposes and the reason for the decision.

Breach of these AISRs shall be considered as a material breach of the Service Agreement and shall be subject to the termination provisions of the Service Agreement in respect of material breach.

8. INTELLECTUAL PROPERTY:

a. Intellectual Property or any output (in whatever form) which is produced or developed or modified by Service Provider during the performance of and/or as a result of Services performed for Alcon pursuant to this Agreement constitutes "Work Product". Unless otherwise specifically agreed the Service Agreement, Alcon shall be the sole owner of, and shall be entitled to use and commercially exploit, at its sole discretion, any and all Work Product. Service Provider shall treat as strictly confidential any and all Work Product. In case of Service Provider use his/her own material without change or critical change input from Alcon. This is not considering a Work Product and therefore Service Provider still have ownership of their Intellectual Property right.

b. Upon completion of any respective Services, or the early termination or expiration of this Agreement, Service Provider shall provide to Alcon all Work Product.

c. Except for the rights specifically granted herein, each party shall retain its respective Intellectual Property Rights owned by them prior to the Effective Date of the Service Agreement. All Intellectual Property Rights, in any form whatsoever, which is owned by or licensed to the Receiver prior to being provided to Service Provider, shall remain the property of the Receiver ("**Alcon Intellectual Property**") and all Alcon Confidential Information shall remain the property of the Receiver or the Receiver's licensor, as the case may be, which shall have and retain all Intellectual Property Rights therein. Service Provider shall acquire no right, title or interest in the Alcon Intellectual Property as a result of its performance of the Services, and it shall not use any Alcon Intellectual Property or Alcon Confidential Information for any purpose other than the performance of Services.

d. Ownership of such intellectual property existing as of the effective date hereof and developed by Service Provider, independent of the Receiver provided Confidential Information and Alcon Intellectual Property **(**"**Service Provider Intellectual Property**"), shall not be affected by the Agreement and the Receiver shall not have any claims to or rights in any Service Provider Intellectual Property, except for the rights granted herein.

e. The designs, images, artwork and other Intellectual Property Rights of a third party obtained by Service Provider for the execution of this project shall belong to the owner of such Intellectual Property Rights. Neither Service Provider nor the Receiver shall have any right over such Intellectual Property Rights.

f. Neither party shall reverse engineer, de-scramble nor de-compile the other party's Intellectual Property Rights.

g. Neither party shall attempt to interfere with the functioning of other party's Intellectual Property Rights and, in particular, shall not attempt to circumvent security, tamper with, hack into, or otherwise disrupt any computer system, database, server, website, router or any other Internet connected device or use automated retrieval devices (such as web robots, wanderers, crawlers, spiders or similar devices) to access information of the other party's Intellectual Property Rights or for any other purpose.

h. Upon the request of the Receiver, after completion of the Services, or the early termination or expiration of the Service Agreement, the Service Provider shall return to the Receiver all Alcon Intellectual Property Rights and Deliverables.

i. Notwithstanding anything contained in the Service Agreement, the Service Provider represents that it owns or has the right to use the Service Provider's Intellectual Property to perform the Services pursuant to the Service Agreement.

9. OBLIGATIONS, REPRESENTATIONS, WARRANTIES AND UNDERTAKINGS:

a. Service Provider shall make its own arrangements for the engagement of its personnel, local or otherwise, and for their transport, housing and payment. Service Provider shall employ technically qualified and competent personnel. All personnel engaged by the Service Provider shall be and remain the full time employees of Service Provider and no claim shall lie against the Receiver in respect of any right or benefit due to them in their employment.

b. Service Provider shall be solely responsible for the supervision and control of its employees/personnel, their safety, security, proper behavior and conduct. Service Provider shall verify the antecedents of employees/agents/authorized representatives/personnel engaged by it for carrying out its obligations under the Agreement.

c. Service Provider shall ensure that its employees/agents/authorized representatives/personnel shall at all times conduct themselves within the parameters of laws and shall not commit, abet or permit the commission of any illegal act, damage, distortion of documents and information while working in the course of the Service Agreement and in the event of any illegal act as herein being committed or abetted, Service Provider shall hold the Receiver indemnified and Service Provider shall be liable for all consequences thereof and the Receiver shall not be liable either directly or indirectly.

d. The Receiver shall in no event and under no circumstances, be liable or responsible for any default by way of non-observance/non-compliance of the said law/rules on Service Provider's part and it shall indemnify the Receiver against any liabilities and costs/expenses from all proceedings in respect thereof.

e. Service Provider shall submit all statutory compliance details/reports if so required by the Receiver.

f. Service Provider hereby represents warrants and covenants that:

(a) It has the necessary power and authority to enter into the Service Agreement and to perform Services contemplated hereunder and to abide by the duties and obligations to be complied hereunder;

(c) It shall perform the obligations contemplated in the Service Agreement in a prudent and professional manner with reasonable care and competence;

(d) It shall at all times conduct itself in accordance with and act within the parameters of law and in accordance with the terms of the Service Agreement.

(e) Perform its obligations under the Service Agreement with high ethical and moral business and personal integrity standards.

g. Service Provider represents warrants and covenants that it shall inform the Receiver of any material change to the original information provided by it to the Receiver at the time of evaluation of its proposal by the Receiver.

h. Service Provider represents and warrants that it shall be liable for all acts of omission, error, commission performed by any employee or collaborator of Service Provider, whether or not the activity is covered under the scope of Services under the Service Agreement, contrary to the directives of the Receiver.

i. Service Provider represents and warrants that the Service Provider is and shall remain, for the term of the Service Agreement and any extension thereof, free from any commitments or conflicts of interest that would impair the Service Provider from rendering its undivided loyalty to the Receiver and/or providing the Services contemplated hereunder in an accurate and timely manner.

10. PUBLICATIONS AND PUBLICITY:

a. Service Provider shall not make any publication, lecture, manuscript, poster presentation or other disclosure or dissemination (oral or written) containing information or referring to the services or deliverables or identifying the Receiver as recipient of these services, either during the term of the Service Agreement or after its early termination or expiration, without the prior written approval of the Receiver.

b. Service Provider shall not disclose the details of the Service Agreement to any third party by any means whatsoever, without the prior written permission of the Receiver.

c. Service Provider shall not use or authorize others to use the name, symbols, or marks of the Receiver in any advertising or publicity material or make any form of representation or statement with regard to Services which would constitute an express or implied endorsement by Service Provider of any commercial product or service without the Receiver's prior written approval.

11. COMPLIANCE WITH LAW AND ALCON GUIDELINES:

a. Service Provider shall at its own cost and at all times in providing the services contemplated hereunder, strictly comply with all applicable laws, without prejudice to the generality of the foregoing provisions relating to the due and proper performance of its duties and obligations under the Service Agreement. In the event of Service Provider committing a breach of this Section 11, it expressly assumes its responsibility for all penalties, liabilities and damages occasioned by the violation of or non-compliance with any such laws or regulations and it also agrees and undertakes to indemnify and keep indemnified the Receiver of, from and against all claims, demands, actions, proceedings, fines, penalties and expenses of whatsoever nature that may be brought against, sustained or incurred by the Receiver and paid for, arising out of or as a result of such breach by the Service Provider. Service Provider agrees to provide a confirmation to the Receiver on compliance with the terms of the Service Agreement as and when required in a format provided by the Receiver from time to time.

b. Service Provider shall obtain and have renewed from time to time all such licenses, permissions or approvals as may be necessary or desirable for providing Services to the Receiver hereunder.

C. Service Provider, its employees and any sub-contractor retained by it shall be bound by Alcon Third Party Code, and any other policies and guidelines that may be provided by the Receiver from time to time and as may be amended.

d. While on the Receiver premises, Service Provider's personnel and any sub-contractor retained by Service Provider for the provision of Services shall observe all regulations of the Receiver regarding the conduct on site and shall otherwise conduct themselves in a business-like manner. If any individual

does not fully comply with such rules or otherwise behave inappropriately, Service Provider shall, upon the Receiver's request, promptly replace such individual without cost to the Receiver.

e. Service Provider will ensure wherever applicable, compliance Alcon Policy on Professional Practices as in force from time to time. Service Provider shall be responsible for training its employees who are involved with performing the Services set forth in the Service Agreement on Alcon Policy at its own expense.

F. Service Provider's breach of any obligation set forth in this Section 11 shall be deemed to be a material breach of the Agreement, and the Receiver shall have the right to immediately terminate the Service Agreement in accordance with Section 4 (Termination).

12. ALCON ANTI BRIBERY GUIDELINES:

In exercising its rights and performing its obligations under the Service Agreement, the Service Provider shall:

a. Comply with all Applicable Laws and regulations; including those related to bribery and anti-corruption;

b. Comply with industry standards;

c. Not promise, offer, pay, cause to pay, accept payment or induce payment or take any action that could be considered a bribe;

d. Comply with all policies and guidelines provided to it by the Receiver in relation to the Service Provider's activities under the Service Agreement, and as amended from time to time. In the event that the Receiver issues additional guidelines or policies in relation to the Service Provider's activities under the Service Agreement, the Receiver will provide the Service Provider with a copy and the Service Provider will duly comply with such guidelines and policies thereafter. Service Provider hereby confirms that it has read and understood the above mentioned Alcon's policies and guidelines; and

e. Perform its obligations under the Service Agreement with high ethical and moral business and personal integrity standards; and

f. Service Provider shall be responsible for training its employees who are involved with the activities set forth in the Agreement and this General Terms and Conditions on anti-bribery at its own expense. Such training shall include the provisions of the applicable anti-corruption laws and the standards. Upon request from the Receiver, Service Provider shall promptly provide a copy of the training material and the training attendance sheets (including name and qualification of the trainer) in respect of training conducted. In addition, if required by the Receiver, Service Provider shall make available its employees, who are involved with the activities set forth in the Service Agreement, to attend or undergo any training conducted by the Receiver on anti-bribery.

13. ALCON RESPONSIBLE PROCUREMENT:

a. The Receiver promotes the societal and environmental values of the United Nations Global Compact. The Receiver expects suppliers with whom we work to comply with the law and to adhere to the Alcon Third Party Code (the "Code") found at https://www.alcon.com/sites/g/files/rbvwei496/files/2019-04/Alcon%20Third%20Party%20Code_V3_11.03.2019.pdf

b. Service Provider agrees and undertakes to:

a) Familiarize itself and comply with the requirements of the Code;
b) Provide information on request to the Receiver concerning compliance with the Code;
c) Allow the Receiver (or its nominated third party experts) adequate access for the purposes of auditing compliance with the Code; and
d) Use its best efforts to rectify identified non-compliances with the Code and report remediation progress to the Receiver on request.

c. Failure to adhere to these standards shall entitle the Receiver to terminate the Service Agreement without compensation.

14. BUSINESS CONTINUITY PLANNING:

a. The Service Provider represents and warrants that it has developed and implemented an effective, written business continuity plan ("BCP") that will ensure that Service Provider is able to continue to provide Services when the Services are interrupted for any reason outside of Service Provider's reasonable control other than force majeure. The Service Provider shall maintain and update the BCP at least annually during the term of the Service Agreement. The Service Provider agrees to put the BCP in effect upon notice from the Receiver, if Service Provider is unable to provide the Services and the Receiver in its sole discretion determines that Service Provider's inability to provide the Services shall have a detrimental impact on the Receiver, then in that event, the Receiver shall have the right to terminate the Service Agreement forthwith upon notice.

b. The BCP shall contain provisions for (a) a risk assessment and business impact analysis, (b) a prevention/mitigation plan and (c) a resumption of Services plan, including a recovery/restoration plan. Such provisions shall include, but not be limited to, (i) Services documentation storage and protection (including, but not limited, to storage of design documents, tools, process and fixtures), (ii) information systems security and redundancy and (iii) demonstrating Service Provider's ability to rapidly recover the loss of capability to deliver Services.

c. The Service Provider shall provide a copy of its then-current BCP within a period of (ten) 10 calendar days of the Receiver's request for the BCP. Alternatively, the Service Provider shall allow any person nominated by the Receiver to inspect the BCP at the premises of the Service Provider.

d. The Service Provider's implementation of the BCP to provide Services shall be at no cost to the Receiver.

e. At the Receiver's request and at no charge, the Service Provider shall participate in any tests implemented by the Receiver or discussions initiated by the Receiver for purposes of evaluating, coordinating and integrating the business continuity plans of its suppliers with the Receiver's overall business continuity plan.

Part-3

Other Terms

15. BLANKET ORDERS AND RELEASES:

a. To make a purchase under the Service Agreement, Parties may enter a Service Agreement defining the scope and the service performance standards and capture the Service Fee and terms pertaining to payment. Any act of acceptance, acknowledgement or of performance under the Service Agreement by Service Provider, would constitute acceptance of the terms by Service Provider. Service provider shall provide Services specified in the Service Agreement in a timely manner and to the satisfaction of the Receiver.

16. REPORTS AND AUDIT:

a. On an agreed date and in an agreed format, Service Provider shall provide the Receiver with such reports in the format and the manner indicated by the Receiver from time to time.

b. The Receiver shall have the right, at its cost, at any time upon reasonable prior notice, to audit all of Service Provider's books and records to ensure its compliance with the Service Agreement, including compliance with Section 11 and 12, and to confirm all payments received from the Receiver. the Receiver may appoint an auditor to perform an audit and, if so, the appointed auditor will be subject to confidentiality obligations in relation to its review of the Service Provider's Confidential

Information. Upon written notice by the Receiver that it wishes to conduct an audit, Service Provider will promptly provide full cooperation and grant access to all relevant documents and materials as reasonably required.

17. MISCELLANEOUS:

a. **Assignment -** The Agreement shall not be assignable by Service Provider in whole or in part without the prior written consent of the Receiver. the Receiver alone shall be entitled to assign the Agreement or any rights and obligations pertaining to the Service Agreement to any of its affiliates or to a Receiver taking over all or substantially all of its business. Any attempted assignment, delegation or transfer in breach of this Section 17 shall be null and void.

b. **Sub-Contracting -** Service Provider shall itself perform the Services and all obligation and duties under the Agreement. Service Provider shall not subcontract or sub license any part of the services without the prior written approval of the Receiver. Such approval, if given, shall not relieve Service Provider from any liability or obligation under the Agreement and Service Provider shall be responsible for the acts, defaults and neglects of itself and any sub-contractor, and their respective agents, servants or workmen as fully as if they were the acts, defaults or neglects of Service Provider. Service Provider will be exclusively responsible for all costs associated with any such sub-license or sub-contract arrangement. Service Provider shall, and shall require all Service Provider sub-contractors to, enter into written Service Agreement containing confidentiality provisions and such other assignments of intellectual property rights as are reasonably required consistent with the Agreement, reasonably cooperate within the scope of Services with the Receiver at no additional cost or charge. The above responsibility of Service Provider to the Receiver shall remain unaffected. Service Provider shall be responsible for all payments to the sub-contractors. Service Provider shall ensure that any entity to which Service Provider sub-contracts or delegates any performance of the services or any obligations under the Service Agreement complies with the Service Agreement.

c. **Severability** - Should one or more of the provisions of the Agreement become void or unenforceable as a matter of law, then the Agreement (including this General Terms and Conditions) will be construed as if such provision were not contained herein and the remainder of the Agreement will remain in full force and effect. Parties shall use their best efforts to substitute for the invalid or unenforceable provision a valid and enforceable provision which conforms as nearly as possible to the original intent of the parties.

d. **Notices**

(a) All notices, consents, waivers, and other communications under this Agreement must be in writing.

(b) Unless otherwise specified by the Service Provider, any notice required to be served by either party to the other shall be served at the address mentioned in the Service Agreement

(c) Any notice required or authorized to be served hereunder shall be deemed to have been properly served if delivered by hand, or sent by registered or certified mail, or sent by facsimile transmission confirmed by registered or certified mail, to the Party to be served at the address specified in the Service Agreement.

(d) Notices sent by post shall be deemed to have been delivered within a period of seven (7) days after the date of posting. Notices sent by facsimile shall be deemed to have been delivered within 24 hours of the time of transmission.

e. **Waivers** - Neither party shall be deemed to have waived its rights under the Agreement unless such waiver is in writing and signed by such Party and such waiver by one party of a breach of any

provision of the Agreement by the other Party shall not be deemed to be a waiver of any subsequent or continuing breach of such provision or of the breach of any other provision of the Agreement by that other Party. Any delay or omission on the part of any Party in the exercise of its strict rights hereunder will not impair those rights nor will it constitute a renunciation or waiver of those rights. All rights, remedies, undertakings, obligations and arrangements contained in the Agreement shall be cumulative, and none of them shall be a limitation of any other right, remedy, undertaking, obligation, or arrangement of any of the parties.

f. Force Majeure

I. Neither Party shall be liable to the other Party for any failure to perform any obligation on its part hereunder to the extent that such failure is due to circumstances beyond its control which it could not have avoided by the exercise of reasonable diligence. The affected Party shall however notify the other Party as soon as practicable of the occurrence of any such circumstance, and the Parties shall meet to consider what steps, if any, can be taken to overcome any issues.

II. Without prejudice to the generality of the foregoing, the following shall be regarded as causes beyond the Service Provider's reasonable control ("Force Majeure Event"):-

a. act of God, explosion, flood, tempest, fire or accident;
b. war or threat of war, sabotage, insurrection, civil disturbance or requisition;
c. acts, restrictions, regulations, bye-laws, prohibitions or measures of any kind on the part of any governmental, parliamentary or local authority;
d. import or export regulations or embargoes;
e. strikes, lock-outs or other industrial actions or trade disputes (whether involving employees of the Service Provider or of a third party).

III. If the Force Majeure Event continues for more than 10 days, the Receiver shall have the right to terminate the Agreement forthwith.

IV. Alternate Source. If any Force Majeure Event prevents, hinders or delays performance of a Service for more than the applicable recovery time objective set forth in the BCP (or, if no time frame is specified, more than 30 days after the date of such event), the Receiver may authorize to procure such Services from an alternate source, or perform such Services for itself solely at the Receiver's cost. In the event the Receiver has already made advance payments for the services yet to be performed, such portion of payment for the services that remain affected/un-delivered due to the force majeure situation shall be refunded immediately to the Receiver.

g. **Relationship between the Parties -** Nothing in the Service Agreement will be construed to ascribe to Service Provider a status other than that of independent contractor. All staff, agents or associates of Service Provider will not be construed as Alcon's employees for any purpose whatsoever. Nothing in the Service Agreement shall in any way be construed to constitute Service Provider as the agent, employee or representative of Alcon or any Affiliate of Alcon. Service Provider shall not have the power to bind Alcon or its Affiliates in any capacity unless specifically authorized to do so by Alcon in writing.

h. **Adverse Event** - Any adverse events, device malfunctions or quality complaints related to the Receiver products should be dealt in accordance with local legal requirements. Service Provider shall forward to the Receiver's local vigilance representative, any vigilance related information, as soon as possible, at the Receiver's address listed in the Service Agreement. In case the Service Provider is conducting Market research activities for the Receiver, the Service Provider is required to comply with

the terms in **Exhibit 1**. In case the Service Provider is involved in the activities of handling, posting, reposting on Social Media on behalf of the Receiver, then the Service Provider is required to comply with the terms in **Exhibit 2**.

EXHIBIT 1

Adverse Events

Adverse Event (AE) is any untoward medical occurrence in a patient or clinical-trial subject administered a medicinal product/ Alcon Medical Device and which does not necessarily have to have a causal relationship with this treatment. An adverse event can therefore be any unfavourable and unintended sign (e.g. an abnormal laboratory finding), symptom, or disease temporally associated with the use of a medicinal product, whether or not considered related to the medicinal product.

Product Complaint

A complaint is any oral, electronic, or written communication that alleges deficiencies related to the identity (labelling), quality, durability, reliability, safety, effectiveness, or performance of a marketed product, including failure of the product, labelling or packaging to meet specifications, whether or not the product is related to or caused the alleged deficiency.

Examples of product/device complaints include but are not limited to:

Product dissatisfaction, Torn contact lenses, Lenses filmy, product not cleaning lenses, Broken haptic on an intraocular lens etc.

Medical Device Malfunction

It is the failure of a device to meet its performance specifications or otherwise perform as intended. Performance specifications include all claims made in the labelling of the device. The intended performance of the device refers to the intended use for which the device is labelled or marketed.

In addition, all special scenarios and other reportable situations, including but not limited to product complaints, medical device malfunctions, as described in the Complaint and Adverse Event training for Customer Oriented Marketing Program (COMPs), must be notified to Alcon.

Hereafter adverse events, special scenarios, Product Complaints and other reportable situations are collectively referred as “AEs” in the Agreement.

Adverse Event Reporting

If Service Provider learns of an AEs in patient(s) in relation of use of a Alcon Medical Device(s) it shall report such incident to Alcon within one calendar day as defined in the Complaint and Adverse Event training for Customer Oriented Marketing Program (COMPs). The Service Provider must report all AEs regardless of the causality or seriousness assessment, product labelling and/or reporter type. Service Provider will notify by using Alcon Complaint Form provided by Alcon to report the event to Alcon. Each report will include information that it is originated from Customer Oriented Marketing Program (COMPs) and is submitted by Service Provider.

Service Provider shall provide Alcon with any and all appropriate personal health information necessary for Alcon to record and report Adverse Event(s) in accordance with applicable law and regulations.

Adverse Event Training

Complaint and Adverse Event training for Customer Oriented Marketing Program (COMPs) must be completed prior to starting any fieldwork or contacting with the participant; then refresher training on annual basis will be provided. In relation to Alcon Medical Devices, training, adverse event identification and reporting, Alcon shall provide Complaint and Adverse Event training to Service Provider employees identified as being directly involved in the Customer Oriented Marketing Program (COMPs). Service Provider shall work with Alcon to ensure that the training is conducted in a timely manner. After receiving Complaint and Adverse Event training the trained employee of the Service Provider may provide training (including the initial training and the annual refresher training) to its employees.

Service Provider shall document the training and archive training records of all involved employees. All training material and documentation shall be made available to Alcon upon request.

Should Service Provider subcontract its work, it is the responsibility of Service Provider to provide training to its subcontractors and ensure compliance with this pharmacovigilance requirement.

Commencement of work

Service Provider shall only start fieldwork or contacting participants when this expressively requested from Alcon.

Service Provider shall report the Program Start Date and Program End Date in writing within 2 (two) days to Alcon.

Adverse Event Reconciliation (AER)

Adverse Event and Product Complaints Reconciliation is a mandatory quality control measure to ensure that during the program all AEs and product complaints have been detected, reported and received by Alcon. AER is scheduled based on the actual Program Start Date and the actual Program End Date.

The process whereby an ESP provides documentation of complaints, adverse events, and events of special interest identified during a COMP to Alcon, and QA Medical Complaint Handling personnel review the appropriate database to assure that all events have been captured.

At the request of Alcon, Service Provider agrees to cooperate and assist Alcon with periodic internal reconciliation efforts to ensure consistency between those AEs and Product Complaints reported by Service Provider during a designated timeframe and those recorded by Alcon as per timeline indicated below (Table 1).

ESP will receive a system notification monthly (last day of the month) to complete and return the Alcon COMP Reconciliation Form to Alcon within 5 days. Alcon will review the information and match with cases received from ESP. Alcon will complete the form with the corresponding case, sign and forward to ESP

Table 1.

Monitoring type	Monitoring periods
AER	Reconciliation takes place monthly for the duration of any COMP.

Audit, Inspection, Corrective Action and Preventive Action

In case of non-compliance with the requirements of the Service Agreement, Service Provider commits to promptly communicating these deviations to Alcon and correct the issues within the mutually agreed timelines.

For the term of the Service Agreement and two (2) years following expiration or termination hereof, Alcon, or its designated third party auditor, shall have the right, to audit Service Provider's (or its agents or subcontractors) processes, procedures and training, including records, data, documentation with respect to AEs in relation of use of Alcon product(s). Service Provider commits to correcting issues from audit observations within the mutually agreed timelines and promptly communicating the actions to Alcon.

In the event of Alcon legal matters, including civil litigation and governmental investigations, or any governmental inspection or audit Service Provider, agrees that it will cooperate as requested. In addition, the Service Provider agrees to allow domestic and international health authorities to inspect their pharmacovigilance operations as it is necessary for Alcon to maintain registration in the countries where the Alcon product is marketed.

Archiving

Service Provider shall also create and archive documents such as AE/Product Complaint reports and forms sent to Alcon during the Term, as well as internal standard operating procedures (SOPs) for its AE/Product Complaint reporting procedures and any COMPs related document including but not limited to source data records from the interaction with participants and maintain them *according to local law/legislation. If local law/legislation is not available, documents must be retained until program closure and a further five years*. Such documents shall be subject to audit.

Alcon reserves the right to amend the Service Agreement at any time if a requirement is imposed upon by an authority or, in its sole clinical discretion, such amendment is necessary for medical safety. Upon written notice from Alcon of any such amendment, Service Provider will comply immediately and any failure to comply shall be deemed as a breach of the Service Agreement.

In the event of any changes in the Service Provider's including, but not limited to: organization name change, service capabilities or operations, the Service Provider must inform Alcon in writing about such changes.

EXHIBIT 2

SOCIAL MEDIA STANDARD PROGRAM / SOCIAL MEDIA LISTENING PROGRAM / THIRD-PARTY SOCIAL MEDIA PROGRAM / MOBILE APPS /WEBSITES

STANDARD PV PROVISIONS

Adverse Event Monitoring: Monitoring of a Social Media Standard (SMS) / Third-Party Social Media (TPSM) program has to occur on business days, twice a day (with at least 8hour between monitoring checkpoints). Monitoring duration of TPSM programs must be performed for the period of the contract / Service Agreement or 60 days after the last sponsored activity, whichever is longer. Monitoring of Digital Assets (i.e. Websites / Mobile Apps) has to occur at a minimum on a daily basis, including weekends and public holidays.

Source Data Verification (SDV): Source Data Verification consists of a check of posts / comments / audio
records on the SM program to confirm that all AEs have been correctly detected and sent to Alcon within twenty-four (24) hours of posting. At a given time the Vendor will be requested to provide the source data to Alcon. The amount of data being checked depends on the number of posts / comments / audio records expected for the SM program. Vendor must send requested posts / comments / audio records to Alcon within a six (6) week time period from the cut-off date of the scheduled due date.

Alcon will have the right to review Vendor source data records for the purpose of determining ESP compliance and accuracy in AE gathering and reporting.

Adverse Event Training. Prior to (i) the Effective Date of the Service Agreement or (ii) with the addition of a new Alcon product under the Service Agreement, as the case may be, and without affecting Vendor's obligations to comply with the Service Agreement and any applicable laws, rules or regulations with respect to AEs, Alcon or an authorized third party agent of Alcon shall provide Vendor employees and / or agents identified by Vendor as being involved with the Alcon products with information and training with respect to AE recognition, identification and reporting. Vendor shall ensure timely distribution of information and work with Alcon to ensure the timely conduct of such training. After such Alcon training and without limiting Vendor's obligations to hire and train its employees to perform the obligations of Vendor under the Service Agreement in accordance with the terms and conditions of the Service Agreement, Vendor shall properly and appropriately update and provide ongoing training to all employees and / or agents of Vendor involved with the Alcon products at least once per annum during the Term (including performing the initial training for new employees or agents hired after the date of Alcon' training) before they are permitted to be involved with the Alcon product(s). Vendor shall record and maintain documentation with respect to training of all such employees and agents and such information and documentation shall be available to Alcon upon request. Should Vendor subcontract out work to other ESPs, it is the responsibility of Vendor to provide training to its subcontractors and ensure compliance by its subcontractors with the Service Agreement.

Record retention: Vendor shall also create, document and maintain for the Term of the Service Agreement and five (5) years thereafter, records of the AE reports and forms sent to Alcon during the Term, and any SMS / SML / TPSM or Mobile App/Website related document including but not limited to source data records [according to local law/legislation]. Such documents shall be subject to audit by Alcon as set forth below.

Corrective Action and Preventive Action, Audit and Inspection. In case of noncompliance with the requirements of the PV Provisions, Vendor commits to promptly communicate these findings to Alcon and discuss corrective and preventive actions to be taken with Alcon. Vendor commits to correct such findings with mutually agreed timelines. For the term of the Service Agreement and two (2) years following expiration or termination hereof, Alcon, or its designated third party auditor, shall have the right, upon reasonable prior advance written notice to Vendor, to inspect and audit Vendor processes, procedures and training, including records and documentation thereof, with respect to AEs, as well as any other information, data or materials in the possession of Vendor (or its agents or subcontractors) related to AEs in patients taking Alcon product(s). Such audits may be scheduled no more frequently than once per year. Vendor shall ensure that any affiliate or agent of Vendor that may have information, data or materials related to AEs, in patients taking a Alcon product(s), or may receive such AEs, is subject to the same obligations and requirements as set forth in this section. The records, documentation, materials and information that are the subject matter of any such audit shall be considered Confidential Information of Vendor pursuant and subject to the provisions of the Service Agreement. To the extent any such audit includes findings of noncompliance with the requirements of the Service Agreement; Vendor commits to correct such audit findings with mutually agreed timelines and promptly communicate corrective actions taken to Alcon. Notwithstanding anything herein to the contrary, in the event Alcon reasonably believes that Vendor has breached its obligations under this Section, or has failed to take appropriate corrective action in response to prior audit findings, Alcon or an independent third party may perform an audit directed at the suspected breach or failure to implement correction by providing Vendor with reasonable prior advance written notice. If Alcon undergoes any type of governmental and/or regulatory inspection or audit, including but not limited to civil litigation related to the subject matter of the Service Agreement, Vendor agrees to reasonably cooperate as requested with respect to such matter. In addition, the Vendor agrees to allow domestic and international health authorities to inspect their pharmacovigilance operations as it is necessary for Alcon to maintain registration in the countries where the Alcon Product is marketed. Alcon reserves the right to amend this Section, at any time if a requirement is imposed upon it by an entity with authority or, in its sole clinical discretion, such amendment is necessary for medical safety. Upon written notice from Alcon of any such amendment, Vendor will comply immediately and any failure to comply shall be deemed a breach of the Service Agreement.

For purposes of the Service Agreement, an Adverse Event is any untoward medical occurrence in a patient or clinical-trial subject administered a Alcon product and which does not necessarily have to have a causal relationship with this treatment. An AE can therefore be any unfavorable and unintended sign (e.g. an abnormal laboratory finding), symptom, or disease temporally associated with the use of a medicinal product, whether or not considered related to the medicinal product. In addition, all cases described as special scenarios, Medical Device Related AEs/incidents, Product Technical Complaints and product specific scenario, in the Alcon AE training for SM programs/Alcon AE training for Public Websites and Mobile Apps that Vendor may be aware of must be notified to Alcon.

Abbreviation List

AE - Adverse Event
App - Application
ESP - External Service Provider
DA - Digital Asset
DAO - Digital Asset Owner
FRM - Form
PSI - Patient Safety Information
PV - Pharmacovigilance
SM - Social media
SML - Social Media Listening
SMS - Social Media Standard
TPSM - Third-Party Social Media

EXHIBIT 3

DATA TRANSFER AGREEMENT

The European Union's (EU) Data Protection Directive 95/46/EC, which has been implemented into national law by each of the Member States of the EU, provides that where the processing of Personal Data is carried out by a Processor on behalf of a Controller established in the EU, Processor must enter into a written contract by which it agrees (i) to act only on the instructions of Controller, (ii) to ensure that appropriate technical and organizational security measures are in place to protect the Personal Data, and (iii) to comply with other appropriate obligations.

Alcon Group Companies have engaged the services of Alcon to process Personal Data as Sub-processor under an Intra Group Data Transfer Agreement. Under the Intra Group Data Transfer Agreement, Alcon Group Companies are the Controller of all Data processed by Alcon and is authorized by mandate to enter into processing or sub-processing agreements on behalf of the other Data Controllers entities within the Alcon group. Alcon is a Processor and Sub-processor acting on behalf of Alcon Group Companies with respect to all Data processed under the master processing agreement.

Alcon has been permitted to appoint Sub-processor(s) subject to certain conditions including, prior permission of Alcon Group Companies and by signing a written contract by which Sub-processor agrees (i) to act only on the instructions of Controller, (ii) to ensure that appropriate technical and organizational security measures are in place to protect the Personal Data, and (iii) to comply with other appropriate obligations.

Alcon and the Service Provider therefore has agreed to sign the Standard Contractual Clauses below to govern Service Provider's processing of Personal Data.

Standard Contractual Clauses (processors)

Clause 1

Details of the transfer

The details of the transfer and in particular the special categories of personal data forms an integral part of the Clauses.

Clause 2

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 3(b) to (i), Clause 4(a) to (e), and (g) to (j), Clause 5(1) and (2), Clause 6, Clause 7(2), and Clauses 8 to 11 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 4(a) to (e) and (g), Clause 5, Clause 6, Clause 7(2), and Clauses 8 to 11, 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 subprocessor this Clause, Clause 4(a) to (e) and (g), Clause 5, Clause 6, Clause 7(2), and Clauses 8 to 11, 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 subprocessor 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 3

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 organisational security measures;

(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, unauthorised 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 subprocessor pursuant to Clause 4(b) and Clause 7(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 and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 10 by a subprocessor 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 3(a) to (i).

Clause 4

Obligations of the data importer

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 organisational security measures 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 unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, 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;

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

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 10;

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

Clause 5

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 2 or in Clause 10 by any party or subprocessor 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 subprocessor of any of their obligations referred to in Clause 2 or in Clause 10, 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 or 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 subprocessor 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, arising out of a breach by the subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 6

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 7

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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 4 (b).

Clause 8

Governing Law

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

Clause 9

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 Clauses.

Clause 10

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 2 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 5 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract 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 subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 4 (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 11

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 subprocessor 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 subprocessor 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.