SANOFI-AVENTIS STANDARD DATA PROCESSING TERMS AND CONDITIONS

***To be read with the Sanofi Purchase Order General Terms and Conditions and/or any other Contract entered into between the Parties**

TABLE OF CONTENTS

1. **RECITAL**

1.1. The Parties hereby agree that in the case of any Purchase Order or ongoing relationship between the Parties, and where the provisions of POPIA apply to the Processing of Personal Information in relation to the Services, these terms and conditions shall apply to and supplement the terms and conditions of such Purchase Order.

1.2. In the event of a conflict between the provisions of this Agreement and the Purchase Order, the provisions of this Agreement will take precedence in regard to all aspects pertaining to any Processing of Personal Information by the Operator of any Data Subjects for the Responsible Party.

2. **DEFINITIONS AND INTERPRETATION**

2.1. "**Agreement**" means this Protection of Personal Information Act Operator terms and conditions;

2.2. "**Affiliate**" means with respect to a Party any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, including Subsidiaries and associates that directly or indirectly, Control, are Controlled by, or are under common Control with a Party. For purposes of this Agreement, the term "Subsidiaries" shall have the meaning ascribed thereto in the *Companies Act, 2008*;

2.3. "**Business Day**" means any day from Monday to Friday and excludes any public holiday as gazetted in the Republic of South Africa;

2.4. "**Confidential Information**" means any information or data of any nature, tangible or intangible, oral or in writing and in any format or medium, which (i) by its nature or content is, or ought reasonably to be identifiable as, confidential and/or proprietary to the Responsible Party or a third party associated to the Responsible Party, or (ii) is provided or disclosed in confidence, and which the Responsible Party or any person acting on behalf of the Responsible Party may disclose to the Operator, or (iii) may come to the knowledge of the Operator by whatsoever means. Without limitation, Confidential Information shall include the following:

2.4.1. information relating to the Responsible Party's business activities, business relationships, products, services, processes, data, and Staff, including agreements to which the Responsible Party is a party (including this Agreement);

2.4.2. information contained in or constituting or relating to the Responsible Party's technology and telecommunications systems including third party hardware and software, and associated material, and information or incidents concerning faults or defects therein;

2.4.3. the Responsible Party's technical, scientific, commercial, financial and market information, methodologies, formulae and trade secret;

2.4.4. the Responsible Party's architectural information, demonstrations, plans, designs, drawings, processes, process maps, functional and technical requirements and specifications and the data relating thereto;

2.4.5. Intellectual property that is proprietary to the Responsible Party or that is proprietary to a third party;

2.4.6. information relating to the Responsible Party's current and existing strategic objectives, strategy documents and plans for both its existing and future information technology, processing, business processing and business process outsourcing; and

2.4.7. Personal Information.

2.5. "**Contract**" means the Purchase Order (read with the Purchase order Terms and Conditions) and any annexures or schedules thereto, or any other written contract entered into between the Parties in respect of the provision of Services by the Operator to the Responsible Party;

2.6. "**Control**" means the ability, by virtue of ownership, right of appointment, voting rights, management agreement, or agreement of any kind, to control or direct, directly or indirectly, the board or executive body or decision making process or management of such entity;

2.7. "**Data Subject**" means any person to whom the specific Personal Information relates, as contemplated in POPIA;

2.8. "**Information Officer**" means the appointed information officer of the Responsible Party, being Ambani Mredlane;

2.9. "**Operator**" has the meaning set out in POPIA ;

2.10. "**Party**" or "**Parties**" means either the Responsible Party or the Operator or both, as the context may require;

2.11. "**Personal Information**" has the meaning set out in section 1 of POPIA, and includes special personal information as defined in section 26 of POPIA and relates only to Personal Information obtained by the Operator as a result of the Contract;

2.12. "**POPIA**" means the *Protection of Personal Information Act, 2013*;

2.13. "**Processing**" has the meaning set out in POPIA and includes any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:

2.13.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.13.2. dissemination by means of transmission, distribution or making available in any other form; or

2.13.3. merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information;

2.14. "**Responsible Party**" has the meaning ascribed thereto in POPIA, and for purposes of this Agreement shall mean Sanofi-Aventis South Africa (Pty) Ltd with registration number 1996/010381/07;

2.15. "**Security Compromise**" means an incident where there has been, or there are reasonable grounds to believe that, Personal Information has been accessed or acquired by an unauthorised person with reference to the Operator's use of the Personal Information under this Agreement;

2.16. "**Services**" means any supply or rendering of services by the Operator for the Responsible Party in terms of a Contract and in terms of which the Operator *inter alia* Processes Personal Information of Data Subjects;

2.17. "**Signature Date**" means the date of signature of the Contract by the last Party to do so in time; and

2.18. "**Staff**" means any employee, independent contractor, agent, consultant, subcontractor or other representative of either Party.

3. **INTERPRETATION**

In this Agreement:

3.1. Words importing:

3.1.1. any one gender includes the other gender;

3.1.2. the singular includes the plural, and vice versa; and

3.1.3. natural persons include created entities (corporate or unincorporated) and vice versa.

3.2. Any reference to "days" shall be construed as being a reference to calendar days unless qualified by the word "business". When any number of days is prescribed in this agreement, same shall be reckoned exclusively of the first and inclusively of the last day unless the last day falls on a Saturday, Sunday or public holiday in the Republic of South Africa, in which case the last day shall be the next succeeding day which is not a Saturday, Sunday or public holiday in the Republic of South Africa.

3.3. The words "include", "includes", and "including" means "include without limitation", "includes without limitation", and "including without limitation". The use of the word "including" followed by a specific example/s shall not be construed as limiting the meaning of the general wording preceding it.

3.4. Any substantive provision, conferring rights or imposing obligations on a Party and appearing in any of the definitions in clause 3 or elsewhere within the Agreement, shall be given effect to as if it were a substantive provision within the body of the Agreement.

3.5. Terms other than those defined in the Agreement and terms appearing in the lower case but which in the title case are defined in the Agreement, will be given their plain English meaning.

3.6. Any Party shall, where relevant, be deemed to be references to, or to include, as appropriate, their respective successors or permitted assigns.

3.7. References to statutory provisions shall be construed as references to those provisions as respectively amended, consolidated, extended or re-enacted from time to time and shall be construed as including references to the corresponding provisions of any earlier legislation directly or indirectly amended, consolidated, extended or replaced by those statutory provisions or re-enacted and shall include any orders, ordinance, regulations, instruments or other subordinate legislation made under the relevant statute.

3.8. Expressions defined in the main body of this Agreement shall bear the same meanings in schedules to this Agreement which do not themselves contain their own conflicting definitions.

3.9. If figures are referred to in numerals and in words in this Agreement and if there is any conflict between the two, the words shall prevail.

4. COMMENCEMENT AND DURATION

This Agreement shall commence on the Signature Date and shall continue to be of force and effect for as long as the Operator remains in possession of any Personal Information of the Data Subjects, regardless of any expiration or termination of a Contract.

5. **PROCESSING BY THE OPERATOR**

5.1. It is recorded that, pursuant to its obligations under this Agreement, the Operator will Process Personal Information of Data Subjects in connection with and for the purposes of the provision of the Services and will act as the Operator for purposes of POPIA.

5.2. The Operator acknowledges and agrees that the Responsible Party retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute the Responsible Party's Confidential Information.

5.3. Unless required by law, the Operator shall Process the Personal Information only:

5.3.1. in compliance with this Agreement; and

5.3.2. for the purposes connected with the provision of the Services or as specifically otherwise instructed or authorised by the Responsible Party in writing.

5.4. If the Operator is ever unsure as to the parameters or lawfulness of the instructions issued by the Responsible Party, the Operator will, as soon as reasonably practicable, revert to the Responsible Party for the purpose of seeking clarification or further instructions.

5.5. The Operator shall co-operate and assist the Responsible Party with consultations with, or notifications to, the relevant regulatory authorities and/or Data Subjects in relation to the Personal Information.

5.6. The Operator shall treat the Personal Information that comes to its knowledge or into its possession as confidential and shall not disclose it without the prior written consent of the Responsible Party, unless required to do so by law.

5.7. Without limiting the Operator's obligations under this Agreement, the Operator shall comply with the Responsible Party’s data privacy and protection policies, applicable industry or professional rules and regulations, in relation to the safeguarding of Personal Information, which may apply to it and take steps to keep abreast and ensure that it and its Staff comply fully with all applicable laws and regulations that are applicable to the Agreement.

6. **SECURITY**

6.1. The Operator undertakes to Process Personal Information in accordance with the Responsible Party's information security and quality measures as set out in Schedule 1 or agreed to by the Parties.

6.2. The Operator shall secure the integrity and confidentiality of Personal Information provided by the Responsible Party by taking appropriate, reasonable technical and organisational measures to prevent:

6.2.1. loss of, damage to or unauthorised destruction of personal information;

6.2.2. unlawful access to or processing of personal information; and

6.2.3. must take reasonable measures to:

6.2.3.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

6.2.3.2. establish and maintain appropriate safeguards against the risks identified;

6.2.3.3. regularly verify that the safeguards are effectively implemented; and

6.2.3.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

6.3. Within 5 (five) Business Days of a request from the Responsible Party, the Operator shall provide to the Responsible Party a written explanation and full details of the technical and organisational measures taken by or on behalf of the Operator to demonstrate and ensure compliance with this clause 6.

7. SECURITY COMPROMISE

7.1. The Operator shall notify the Responsible Party in writing immediately and in any event, no later than 24 (twenty four) hours if there has been a Security Compromise.

7.2. The Operator shall as soon as is reasonably possible investigate the Security Compromise and furnish the Responsible Party with:

7.2.1. a preliminary report within 24 (twenty four) hours from its initial notification to the Responsible Party in terms of clause 7.1 above setting out the details of the Data Subjects affected by the Security Compromise and the nature and extent of the Security Compromise, including details of the identity of the unauthorised person who may have accessed or acquired the Personal Information; and

7.2.2. daily reports on progress made at resolving the compromise.

7.3. The Operator shall take reasonable steps to mitigate the effects and to minimise any damage resulting from the a Security Compromise and assist the Responsible Party in remediating or mitigating any potential damage from the breach to the extent that such remediation or mitigation is within the Operator’s control as well as reasonable steps to prevent a recurrence of such a Security Compromise, including interviewing and the possible removal of staff from the performance of Services for the Responsible Party.

8. **OPERATOR STAFF**

The Operator shall:

8.1. limit the Processing of and access to the Personal Information to those Staff who need to know the Personal Information to enable the Operator to render the Services;

8.2. ensure that its Staff will not Process Personal Information: (i) except in accordance with the provisions of this Agreement; and (ii) procure that its Staff are contractually obligated to maintain the security and confidentiality of any Personal Information and this obligation continues even after their engagement ends; and

8.3. take all reasonable steps to ensure the Staff Processing Personal Information receive adequate training on compliance with this Agreement and POPIA applicable to the Processing.

9. **ACCESS REQUESTS**

9.1. The Operator shall provide the Responsible Party with full cooperation and assistance in relation to any requests for access to, correction of or complaints made by the Data Subjects relating to their Personal Information.

9.2. The Operator shall notify the Responsible Party in writing:

9.2.1. within 3 (three) Business Days of receipt thereof, of any request for access to or correction of the Personal Information or complaints received by the Operator relating to the Responsible Party's obligations in terms of POPIA and provide the Responsible Party with full details of such request or complaint; and

9.2.2. promptly of any legally binding request for disclosure of Personal Information or any other notice or communication that relates to the Processing of the Personal Information from any supervisory or governmental body.

10. **AUDIT RIGHTS**

10.1. The Responsible Party or its agent shall have the right to audit the Operator at any time, with reasonable notice, if there is a reasonable suspicion that the Operator is not complying with the provisions of this Agreement or where there is a suspicion that the confidentiality, integrity and accessibility of Personal Information is likely to be compromised. Such audit rights shall include the right of access to systems, procedures and software, and inspection of the physical security of the Operator's premises.

10.2. The Operator shall offer reasonable assistance and co-operation to the Responsible Party and/or its auditors or inspectors in the carrying out of such auditing exercise.

10.3. To the extent that the Operator engages an independent auditor in relation to the provisions of applicable data privacy and protection legislation to carry out an audit of its operations, the Operator agrees to provide the Responsible Party with copies of the audit reports of all such audit exercises.

10.4. Nothing in this clause 10 should be read as providing the Responsible Party with unlimited access to audit the Operator without just cause.

11. SEPARATION OF PERSONAL INFORMATION

The Operator shall Process the Personal Information in relation to the Services separately from Personal Information, data and property relating to the Operator or any third party, and may not be combined or merged with information of another party unless otherwise agreed to in writing by the Responsible Party.

12. RETURN AND RETENTION OF PERSONAL INFORMATION

12.1. The Responsible Party may, at any time on written request to the Operator, require that the Operator immediately return to it any Personal Information and may, in addition, require that the Operator furnish a written statement to the effect that upon such return, it has not retained in its possession or under its control, whether directly or indirectly, any such Personal Information or material.

12.2. Alternatively, the Operator shall, as and when required by the Responsible Party on written request, destroy all such Personal Information and material and furnish the Responsible Party with a certificate of destruction to the effect that the same has been destroyed, unless the law prohibits the Operator from doing so. In that case, the Operator agrees that it will maintain the confidentiality of the Personal Information and will not actively Process the Personal Information any further.

12.3. The Operator shall comply with any request in terms of this clause 12 within 7 (seven) days of receipt of such request.

13. SUBCONTRACTING

13.1. The Operator may not subcontract the performance of any of its obligations under this Agreement without the Responsible Party's prior written consent having been obtained. All references to the Operator's Staff shall be deemed to include the employees of any subcontractor of the Operator.

13.2. In the event that the Responsible Party agrees to the Operator subcontracting certain or all of the Operator’s obligations, the Operator must only do so by way of a written contract with the subcontractor which contract must impose the same obligations on the subcontractor as are

imposed on the Operator in terms of this Agreement insofar as the Processing of Personal Information by the subcontractor is concerned.

14. **CROSS-BORDER DATA TRANSFER**

14.1. It is hereby recorded and agreed that in order for the Operator to be able to fulfil its obligations in terms of the Contract, it may be necessary for the Operator to transfer Personal Information to a third party outside of South Africa.

14.2. In the event of such cross-border transfer, the Operator hereby warrants and undertakes in favour of the Responsible Party that:

14.2.1. it shall procure the third party's compliance with all the obligations of this Agreement insofar as the Processing of Personal Information by the third party is concerned;

14.2.2. the Operator shall at all times be responsible to the Responsible Party for fulfilment of all the Operator's obligations under the Contract and remain the Responsible Party's sole point of contact regarding the Services, including with respect to payment;

14.2.3. the third party is prevented from further transferring Personal Information to other third parties;

14.2.4. it shall ensure that the third party has implemented the appropriate technical and organisational security measures in the relevant jurisdiction in which the Personal Information is being transferred, as contained in Schedule 1; and

14.2.5. it has implemented and taken technical and organisational security measures to safeguard the security of the Personal information in-transit.

14.3. The Operator hereby agrees that the Responsible Party shall solely hold it responsible for the fulfilment of all obligations under this Agreement and it hereby indemnifies and holds the Responsible Party harmless from any and all losses arising from any claim or action brought against the Responsible Party by any party, including by any regulator, arising from or due to the Operator's or the offshore third party's breach of the obligations contained in this Agreement in relation to the lawful Processing of Personal Information in South Africa or anywhere else in the world.

15. **CONFIDENTIALITY**

15.1. The Operator agrees and undertakes:

15.1.1. except as permitted by this Agreement, not to disclose or publish any Confidential Information in any manner for any reason or purpose whatsoever without the prior written consent of the Responsible Party and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Operator to obtain the consent of such third party;

15.1.2. except as permitted by this Agreement, not to utilise, employ, exploit or in any other manner whatsoever use the Confidential Information for any purpose whatsoever without the prior written consent of the Responsible Party and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Operator to obtain the consent of such third party;

15.1.3. to restrict the dissemination of the Confidential Information to only those of its Staff who are actively involved in activities for which use of Confidential Information is authorised and then only on a "need to know" basis and the Operator shall initiate, maintain and monitor internal security procedures reasonably acceptable to the Responsible Party to prevent unauthorised disclosure by its Staff; and

15.1.4. to take all practical steps, both before and after disclosure, to impress upon its Staff who are given access to Confidential Information the secret and confidential nature thereof.

15.2. The obligations of the Operator with respect to each item of Confidential Information shall endure for an indefinite period from receipt of that item of Confidential Information. The obligations referred to in this clause 15 shall endure notwithstanding any termination of this Agreement, any other agreement entered into between the Parties or any discussions between the Parties.

15.3. The Operator hereby indemnifies and holds the Responsible harmless from any and all losses arising from, or in connection with, any claim or action arising from the Operator's breach of any obligation with respect to Confidential Information.

16. RESPONSIBLE PARTY AFFILIATES

Unless otherwise agreed to the contrary, the Parties hereby agree that any Affiliate of the Responsible Party shall be entitled to rely on all the provisions of this Agreement, which provisions are binding between the Affiliate of the Responsible Party and the Operator, in respect of any contract that might be entered into between the Operator and the Affiliate of the Responsible Party in terms of which the Operator will be Processing Personal Information on behalf of the Affiliate of the Responsible Party. For the avoidance of doubt, this Agreement is applicable and binding in respect of all contracts

concluded between the Operator and the Responsible Party or the Affiliate of the Responsible Party where the Operator Processes Personal Information on behalf of the Responsible Party or the Affiliate of the Responsible Party.

17. **INDEMNITY**

17.1. The Operator hereby indemnifies the Responsible Party in respect of all losses, claims, damages, costs, expenses, fines and penalties arising from and in connection with the Operator's (including its Staff) actions and/or omissions relating to this Agreement.

17.2. Any financial caps or limitation of liability set out in the Contract shall not apply to this indemnity.

18. **BREACH AND TERMINATION**

18.1. In the event of either of the Parties committing a breach of any of the conditions of this Agreement and failing to remedy such breach within 7 (seven) Business Days of receipt of a notice from the other Party requesting it to remedy such breach, then the other Party shall be entitled to cancel this entire Agreement forthwith and claim such losses as it may have suffered. In the event of termination of this Agreement, the Party terminating this Agreement shall have a right to also exercise its rights of termination under the Contract.

18.2. Notwithstanding anything to the contrary contained in this Agreement, the Parties shall be entitled to terminate this Agreement by mutual agreement in writing.

18.3. The provisions of this clause 18 shall not affect or prejudice any other rights/remedies which the Parties may have in law or in any other Contract between the Parties.

19. **CONSEQUENCES OF TERMINATION**

19.1. The termination of this Agreement shall not affect the rights of either of the Parties that accrued before termination of this Agreement or which specifically survives the termination of the Agreement.

19.2. Upon termination of this Agreement or upon request by the Responsible Party, the Operator shall return or destroy any material containing, pertaining or relating to the Personal Information disclosed pursuant to this Agreement to the Responsible Party in terms of clause 12 unless the law prohibits the Operator from doing so. In that case, the Operator agrees that it will maintain the confidentiality of the Personal Information and will not, under any circumstance, Process the Personal Information any further.

20. **WAIVER**

20.1. Failure or delay by either Party in exercising any right will not constitute a waiver of that right.

20.2. No waiver of any of right under this Agreement will be binding unless it is in writing and signed by the Party waiving the right.

21. **SEVERABILITY**

If any part of this Agreement is found to be invalid or unenforceable, it shall be severed from the remainder of this Agreement, which shall remain valid and enforceable.

22. **CESSION AND DELEGATION**

The Operator may not cede its rights or delegate its obligations in terms of this Agreement, without the prior written consent of the Responsible Party, which consent shall not be unreasonably withheld.

23. **GOVERNING LAW AND JURISDICTION**

23.1. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed exclusively in accordance with South African law.

23.2. The Operator consents and submits to the jurisdiction of the High Court of South Africa, Gauteng Local Division, Johannesburg in any dispute arising from or in connection with this Agreement. Without prejudice to any other rights or remedies which the Responsible Party may have, the Operator acknowledges that nothing herein shall preclude the Responsible Party from seeking urgent relief or specific performance from a court of competent jurisdiction.

24. **NOTICES AND *DOMICILIUM***

24.1. The Parties choose the addresses set out in the Contract as their respective *domicilia citandi et executandi* for purposes of giving any legal notice and serving any legal process.

24.2. Any notice addressed to a Party at its physical or postal address shall be sent by prepaid registered post or delivered by hand.

24.3. Any notice shall be deemed to have been given and received:

24.3.1. if posted by prepaid registered post, 7 (seven) days after the date of posting thereof;

24.3.2. if hand delivered, on the day of delivery; and

24.3.3. if sent by email on the first Business Day after the date of transmission.

24.4. Notwithstanding anything to the contrary contained in this clause 24 a written notice or communication actually received by a Party shall constitute adequate written notice or

communication to it notwithstanding that it was not sent or delivered to its chosen *domicilium citandi et executandi* or in the manner provided in this clause 24.

25. **WHOLE AGREEMENT**

This Agreement constitutes the whole of the agreement between the Parties hereto relating to the subject matter hereof and the Parties shall not be bound by any terms, conditions or representations whether written, oral or by conduct and whether express or tacit not recorded herein.

Schedule 1 INFORMATION SECURITY AND QUALITY MEASURES

The Information Security and Quality measures listed in this document are applicable depending on the nature, context and scope of the provided Services (hereinafter, the "**Information Security and Quality Measures**"). By default, the Operator shall ensure compliance with all the Information Security and Quality measures listed in this document.

In the event where the Operator judges that an Information Security and Quality Measure is not applicable to the nature, context and scope of the provided Services, the Operator shall have to justify such non-applicability with written evidence.

1. DEFINITIONS

1.1. Audit Trail: A chronological recording of events, such as creation, modification, deletion of – and access to (GxP or non-GxP) record or e-record, that allows reconstruction of the course of events and indicates who created, accessed, changed or deleted data and why.

1.2. Data Integrity: degree to which a collection of data is managed through effective organizational, operational, and technical mechanisms to ensure data reliability.

1.3. Equipment: all equipment, terminals, infrastructures, related hardware and software, including, as applicable, systems (i.e. any and all IT networks or resources that process, store, support, transmit or contain Responsible Party Data, applications, databases, central processing units, personal computers and other processors, controllers, storage devices, printers, phones, other peripherals and input as well as output devices, and other tangible mechanical and electronic equipment intended for the processing, input, output, storage, manipulation and retrieval of information and Responsible Party Data;

1.4. GxP and Other Health-related Regulations: Regulations such as Good Clinical Practices, Good Laboratory Practices, Good Pharmacovigilance Practices, Good Manufacturing Practices and Good Distribution Practices, as well as any other regulation applicable to the Responsible Party and related to public health;

1.5. GxP Computerized System: Computerized system used in support of a GxP or other health-related regulated activity.

1.6. Incident: any event that does not correspond to a normal process and that could lead to interruption or quality reduction of the Services provided to Responsible Party.

1.7. IT Change: any actual or proposed change to the nature, level and extent/scope of an IT System;

1.8. Responsible Party Data: means, without any limitation, any data (including Personal Data) and associated Audit Trail, records, documents or information of Responsible Party accessed or managed by Operator under the Agreement.

1.9. Security Incident: includes, as further defined in this document, any virus and, without limitation, an actual, suspected, attempted or threatened unauthorized: (i) exposure, access, use, deletion, revision, encryption, reproduction, destruction, loss, theft, alteration, disclosure, copying, modification or transmission regarding any component of Responsible Party Data including users confidential information, which is or should be under control of Operator or for which Operator is responsible, or, as the case may be, (ii) access (physical or otherwise), theft or damage regarding any of the Responsible Party's Equipment controlled by or for Operator or on which Responsible Party Data is processed or stored.

1.10. SOX: Sarbanes-Oxley Act of 2002 also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House) and more commonly called Sarbanes–Oxley, Sarbox or SOX, is a United States federal law that set new or expanded requirements for all U.S. public company boards, management and public accounting firms.

2. INFORMATION SECURITY RESPONSIBILITIES AND OBLIGATIONS

2.1. Information security individual

2.1.1. Operator shall designate an information security responsible individual. The information security responsible individual is considered as the single point of contact for information security topics and shall be in charge of all the security measures listed in this document.

2.1.2. The information security manager in coordination with Operator shall designate a backup assistant in case of absence.

2.2. Information security program

2.2.1. Operator shall maintain, monitor, and as necessary improve and update a comprehensive, written "**Information Security Program**" applicable to the cloud and/or Services as well as to the protection of the security and Data Integrity.

2.2.2. Such Information Security Program shall be reasonably consistent with the industry standards and best practices, and shall contain documented policies and procedures, administrative, technical, and physical safeguards to protect and ensure the security, integrity and confidentiality of the cloud, the Services and Responsible Party Data.

2.3. Security Assurance Plan

In the event where all or part of the Responsible Party's Equipment is outsourced and/or provided by Operator or its authorized subcontractors, Operator shall maintain, monitor, and as necessary improve and update a comprehensive, written "Security Assurance Plan". The Security Assurance Plan shall describe how Operator will implement, when applicable, each security measure listed in this document. The Security Assurance Plan shall be validated by Responsible Party's prior to the performance of the Services.

2.4. Risk assessment program

Operator shall provide and implement a regular assessment of the internal and external risks to the security, confidentiality, integrity and availability of Responsible Party Data, including without limitation identification and evaluation of vulnerabilities to Operator’s Equipment.

2.5. Acceptable use policy

Operator shall institute an acceptable use policy that its Staff shall be aware of before gaining any access Operator's Equipment.

2.6. Security investigations

Operator shall fully cooperate with the Responsible Party in case of any security investigation regarding potential breaches of its information security obligations.

2.7. Security issues notification

Operator shall report to the Responsible any potential security issue regarding Operator's and/or Responsible Party's Equipment or any other event requiring notification under applicable law. Operator shall not exploit or disclose such security issues. The Responsible Party shall be notified within 24 hours of any potential security issue.

2.8. Security Incident management

Operator shall manage and proceed to the mitigation of Security Incidents regarding Operator's Equipment and/or Services provided to the Responsible Party by following an Incident management process and adequate response plan.

2.9. IT Change management

2.9.1. Operator shall follow a formal IT Change management process to control any IT Change which could potentially affect Responsible Party Data integrity, compliance, functionality or availability of Services provided to the Responsible Party.

2.9.2. Operator shall perform IT Changes to Responsible Party Data by using the normal functionality of the Services.

2.9.3. Operator shall provide a dedicated pre-production environment to the Responsible Party to ensure proper testing of IT Changes before release into production.

2.9.4. Operator agrees to provide a 30 days' notice to Responsible Party before any IT Changes that impact directly or indirectly the Services. Regular operations such as maintenance or Incident response are not considered as IT Changes and should follow their dedicated processes.

2.9.5. In case of failures or issues resulting from an IT Change, Operator shall be able to follow a rollback plan so that the Services which are used by or for Responsible Party or Responsible Party Data get back to theirs state before the IT Change.

3. INFRASTRUCTURE SECURITY

3.1. Network security

3.1.1. Operator shall apply best practices in terms of network partitioning to include but not limited to:

3.1.2. Each network shall be isolated from other networks by the use of firewalls; only permitted incoming and/or outgoing communication flows shall be authorized.

3.2. Network protocols protection

Operator shall ensure that all network protocols are secure, current and implemented with no known vulnerabilities.

3.3. Infrastructure hardening

3.3.1. Operator shall ensure that its network key components, network flows and operating systems are hardened. This may include (but not limited to) the following:

3.3.1.1. Network flows shall be filtered, unused or outdated network protocols shall be deactivated.

3.3.1.2. Unused or outdated operating systems services or functions shall be deactivated.

3.3.1.3. Unused or outdated network equipment's services, functions or physical ports shall be deactivated.

3.3.1.4. Default administration and/or connection passwords shall be changed.

3.3.1.5. Software and/or add-on installations shall be strictly controlled.

3.3.1.6. Configuration changes shall be strictly controlled.

3.4. Malware protection

Operator shall ensure that network key components and the Equipment are protected against all types of malware with adequate and updated anti-malware.

3.5. Network documentation

Operator shall ensure that its network architecture is documented.

3.6. Administration platforms protection

Operator shall restrict all remote administration platforms and infrastructure to Operator IP sources addresses.

3.7. Wireless networks protection

3.7.1. Operator shall ensure that its wireless networks are adequately protected. This may include (but not limited to) the following:

3.7.1.1. Wireless access shall be protected with a secure authentication protocol and with adequate key length.

3.7.1.2. Wireless access points emission power shall be correctly dimensioned to Operator area so that wireless cannot be reached from outside Operator area (outside buildings).

3.7.1.3. Wireless access points' default administration credentials and/or connection passwords shall be changed.

3.7.1.4. Unused or outdated wireless access points' services, protocols, functions or physical ports shall be deactivated.

3.7.1.5. Wireless networking devices shall have updated firmware.

3.7.1.6. All wireless connections must be authenticated and authorized.

3.8. Dedicated service and hosting environment

3.8.1. Responsible Party Service environment shall be logically separated from other Operator’s clients under a dedicated server instance.

3.8.2. Responsible Party Data should physically reside in a dedicated database environment under a dedicated database instance.

3.9. Mobile devices protection

3.9.1. In case where Operator’s Staff shall use their own and/or corporate mobile devices for the aim to deliver the Services to the Responsible Party:

3.9.1.1. Operator shall protect its mobile devices with a password. This password must be compliant with the following rules:

3.9.1.1.1. Password length: 8 characters minimum.

3.9.1.1.2. Password timeout: password must be re-entered after 60 minutes of inactivity.

3.9.1.1.3. Password change: password must be changed on a yearly basis.

3.9.1.1.4. Password history: the last two passwords must not be re-used.

3.9.1.2. Operator shall manage and administer its Staff's mobile devices.

3.9.1.3. Operator shall ensure a clear segregation between professional and private applications and data.

3.9.1.4. In the event any Responsible Party Data is stored on any mobile device, such devices shall be in an encrypted form.

3.10. Equipment management program

Operator shall apply best practices in terms of Equipment management regarding its own and Responsible Party managed Equipment.

3.11. Maintenance contracts

Operator shall maintain maintenance contracts with all Equipment’s Operators in terms of information security.

3.12. Teleworking security

Operator shall have a teleworking policy that effectively protects Responsible Party Data and Equipment.

4. ACCESS CONTROL

4.1. Passwords protection

4.1.1. Operator shall ensure that its password policy meets industry standard best practices ("Password Protection Policy" from SANS Institute or "DAT-NT-001/ANSSI/SDE/NP" from ANSSI) for strong password management, including at the minimum (but not limited to):

4.1.1.1. Minimum password length

4.1.1.2. Password complexity

4.1.1.3. Restriction of password reuse

4.1.1.4. Account lockout

4.1.2. Operator shall ensure that passwords are encrypted while transmitted and will be changed at the first connection.

4.1.3. Operator shall ensure that its Staff shall not store or write passwords in clear text.

4.2. Remote access

Operator shall document its remote accesses procedures. Remote accesses shall rely on secure network protocols and shall use two-factor authentication.

4.3. Physical access control to Responsible Party Data

4.3.1. Operator shall implement and maintain reasonable restrictions upon physical access to Responsible Party Data including procedure that sets forth the manner in which physical access is restricted.

4.3.2. Operator shall maintain an Audit Trail of all physical access to the hosting premises of Responsible Party Data.

4.4. Logical access control to Responsible Party Data

4.4.1. In the event where Operator may host, process, transmit or collect Responsible Party Data:

4.4.1.1. Operator shall document, implement, maintain and update adequate security controls to ensure that Operator will never use or access

Responsible Party Data without the explicit request of the Responsible Party or its approval or unless there is a legitimate identified business need validated by the Responsible Party.

4.4.1.2. The logical access credentials to Responsible Party Data shall be strictly limited to authorized Operator's Staff.

4.4.1.3. Operator shall maintain an inventory of all authorized logical access to Responsible Party Data.

4.4.2. Operator shall record the list of its Staff that had / have access to Responsible Party Data via front and back-end access authorizations. Operator shall provide documented evidence on request from the Responsible Party.

4.4.3. Both Operator and Responsible Party shall ensure that (i) only authorized Staff are able to access or use the Services and/or the Responsible Party Data, (ii) creation, change and deactivation of user access authorizations are recorded, (iii) users are effectively trained before to authorize their access requests, (iv) access authorization levels are appropriate with the responsibilities and the role played in the system.

4.5. Logical access control to the Responsible Party network

4.5.1. In the event where Operator's Staff implement, maintain or administer any kind of Equipment remotely:

4.5.1.1. Operator shall document, implement, maintain and update adequate security controls to ensure that its Staff will never access the Responsible Party's Equipment without the explicit request of the Responsible Party or its approval or unless there is a legitimate identified business need validated by Responsible Party.

4.5.1.2. The logical access credentials to the Responsible Party's network shall be strictly limited to authorized Operator's Staff.

4.6. Physical access control to Responsible Party's premises

4.6.1. In the event where the management of the Responsible Party's premises is outsourced by Operator:

4.6.1.1. Operator shall implement and maintain reasonable restrictions upon physical access to the Responsible Party's premises, including procedure that sets forth the manner in which physical access is restricted.

4.6.1.2. Operator shall maintain an Audit Trail of all physical access to the Responsible Party's premises.

4.7. Access logging and monitoring

Operator shall log all activities related to the access to Responsible Party Data, including access requests. Retention period must be in compliance with local regulation and agreement with the Responsible Party.

4.8. Third parties' access

Operator shall not permit any third party to access Responsible Party Data, or environment within Operator or Responsible Party's infrastructure unless written prior authorization by the Responsible Party.

4.9. Permanent Access to Responsible Party Data

Operator shall ensure the Responsible Party access to the Responsible Party Data throughout the duration of the performance of the Services within the format previously agreed with the Responsible Party.

5. APPLICATION SECURITY

5.1. Information security integration into application development

5.1.1. In case where Operator is deemed to be an application's developer/Operator/integrator, Operator shall ensure (but not limited to) the following:

5.1.1.1. Operator shall integrate through all application development life cycle phases information security needs of the application with regards to confidentiality, integrity, availability and traceability aspects.

5.1.1.2. Operator shall rely on Open Web Application Security Project (OWASP)'s best practices in terms of secured application development.

5.1.1.3. Operator shall segregate the application development environment(s) from the application production environment(s).

5.1.1.4. Operator shall ensure access to the development and production environment follows best practices and enforces segregation of duties.

5.1.1.5. Operator shall ensure that application source code has been reviewed and assessed regarding published well known information security source code vulnerabilities.

5.1.1.6. Operator shall strictly control access to application source code.

5.1.1.7. Operator shall perform a vulnerability test on its provided application prior to move to production.

5.1.1.8. Operator shall perform vulnerability tests at least once a year.

5.1.1.9. Operator shall ensure that the test and development environments offer the same level of protection as the production environment.

5.1.1.10. Operator shall ensure that application has the ability to restrict access to Personal Data to authorized users only.

5.1.1.11. Operator shall ensure that application logs all access to Personal Data.

5.2. Application maintenance & support

5.2.1. Operator agrees to provide, maintain and support its application and subsequent updates, upgrades, and bug fixes such that the application is, and remains secure from known vulnerabilities.

5.2.2. Operator agrees to provide at least 30 days' notice to the Responsible Party before updating any of its application which is used by or for Responsible Party or Data.

5.3. Application hardening

5.3.1. Operator shall ensure that its provided application is hardened. This may include (but not limited to) the following:

5.3.1.1. Unused or outdated application's services or functions shall be deactivated.

5.3.1.2. Default administration passwords shall be changed.

5.3.1.3. Whenever possible, application shall not integrate uncontrolled source code, adds-on or plugins.

5.3.1.4. Configuration changes shall be strictly controlled.

5.4. Development data

5.4.1. In case where Operator (or its authorized subcontractors) is deemed to be an application developer/Operator/integrator:

5.4.1.1. Developer shall never use or access Responsible Party Data without the explicit request of the Responsible Party or its approval or unless there is a legitimate identified business need validated by the Responsible Party; and

5.4.1.2. De-identified or representative data shall be used in the development and test environment.

6. RESPONSIBLE PARTY DATA PROTECTION

6.1. Responsible Party Data protection

6.1.1. Operator shall ensure that all Responsible Party Data is encrypted during transmission whether sent over the Internet or otherwise.

6.1.2. Operator shall protect all Responsible Party Data stored on databases, servers, or other forms of non-mobile devices against all reasonably-anticipated forms of compromise, whether by use of encryption, logical access controls, or other robust safeguards.

6.1.3. Responsible Party Personal Data: Where possible, Operator shall either encrypt all Personal Data stored at rest with separate key management or anonymize them entailing that re-identification is not possible.

6.1.4. In the event any Responsible Party Data is stored on any mobile device (including, but not limited to, laptop computers, compact discs, tablet computers, external hard drives, backup tapes and/or removable diskettes), such devices shall be in an encrypted form.

6.2. Responsible Party Data and system configuration backup

6.2.1. Operator shall backup Responsible Party Data, associated Audit Trail and system configuration on a regular basis following industry best practices for backup.

6.2.2. Operator shall perform at least two backup copies onto different physical distant locations.

6.2.3. All backups shall be encrypted.

6.2.4. Operator shall perform a 3 years rotation restore test and provide documented written evidence to Responsible Party.

6.2.5. When a significant IT Change on the computerized system impacts the backup and restore functionality / Services / specifications, Operator shall apply the IT Change Management process (as described in the paragraph dealing with IT Change Management of the present document) must ensure that a new restore test is performed.

6.2.6. Operator shall provide documented evidences upon request from the Responsible Party that backups jobs have started and ended as planned.

6.3. Third parties restriction

No Responsible Party Data shall be sold, assigned, leased to a third party or otherwise disposed of by Operator or commercially exploited by or on behalf of Operator.

7. STAFF SECURITY

7.1. IT segregation of duties

Operator shall implement an information technology segregation of duties. Operator shall segregate its Staff' tasks based on a need to do basis as required by their job responsibilities.

7.2. Information security training and awareness program

During the term of the Agreement, Operator will implement and maintain up to date a training and awareness program for its Staff regarding its information security obligations. In case where Operator collects, provides, stores, transmits or process in any manner Responsible Party Data, this program shall include a section dedicated to Responsible Party Data protection. Operator shall ensure that all its Staff involved in the Services performance will regularly attend such program.

7.3. Operator Staff departure

7.3.1. Upon termination of an Operator's Staff agreement for whatever reason, Operator's shall ensure that Staff's departure is correctly managed in terms of information security.

7.3.2. This may include (but not limited to) the following:

7.3.2.1. All Staff logical and physical credentials have been correctly deactivated.

7.3.2.2. All the Responsible Party's equipment and Data have been returned.

7.3.2.3. If Responsible Party Data have been locally stored for whatever reason on Staff's workstation or mobile device, hard drives and/or storage memories shall be securely wiped.

8. TERMINATION OF THE AGREEMENT

8.1. Responsible Party Data return, destruction or sanitization

Unless otherwise required by law or regulation, upon termination of the Agreement for whatever reason, Operator shall cease processing any Responsible Party Data on behalf of the Responsible Party and, at the Responsible Party's option, shall either return to the Responsible Party all of the Responsible Party Data and any copies thereof which it is processing, has processed or have had processed on behalf of the Responsible Party in a format agreed with the Responsible Party, or destroy the Responsible Party Data if requested by the Responsible Party or sanitize Responsible Party Data from Operator's environment and provide evidence of such sanitization or destruction of Responsible Party Data within 15 days of termination of Agreement.

8.2. Equipment return

Upon termination of the Agreement for whatever reason, all the Responsible Party Equipment shall be returned within 30 days of termination of Agreement.

9. INFORMATION SECURITY AND QUALITY AUDITS AND CONTROLS

9.1. Right to Audit

9.1.1. The Responsible Party or an appointed audit firm by Responsible Party has the right to audit the Operator and carry out any controls it considers useful to ensure the compliance with its Information Security and Quality obligations. To do so, Operator shall allow representatives from the Responsible Party to have access for audit purposes to its related premises and facilities and agree to share documentation and evidence.

9.1.2. In addition, the Responsible Party's shall be authorized to audit Operator’s subcontractors and their systems; this does not release Operator from taking all reasonable steps to verify that its subcontractors comply with the provisions of this document.

9.1.3. The Responsible Party will ensure to cause the least amount of disruption to Operator’s activities.

9.1.4. Such controls shall be carried out as per the provisions of the Agreement.

9.2. Information Security

9.2.1. Annual Information Security Assessment

In addition, each calendar year, Operator shall engage at its cost and expense a nationally-recognized audit firm identified by the Responsible Party or proposed by Operator to conduct an audit which shall cover, at a minimum, Operator’s security policies and procedures and controls, including cloud and data security. Upon Responsible Party's request, Operator shall provide the Responsible Party with a copy of such report.

9.2.2. Remediation Plan

If an audit reveals any breaches or deficiencies pursuant to this Agreement or if the Responsible Party raises recommendations or reservations following an audit, Operator shall promptly and at its sole cost and expense (i) execute a remediation plan to correct those breaches and/or deficiencies and (ii) implement the recommendations and reservations issued by the Responsible Party.

9.3. Quality Audit

9.3.1. As part of pre-selection process and on a routine basis, no more than once a year, Responsible Party may leverage the Right to audit (on site or using a postal audit questionnaire).

9.3.2. Additionally, where significant issues are detected regarding the Services provided by the Operator, the Operator shall authorize the Responsible Party to carry out when needed an audit for cause designed to lead to resolution of these issues.

9.3.3. After provision of an audit report by the Responsible Party, Operator shall respond with correction and/or corrective and preventive action plans to critical findings within fifteen (15) business days of receipt of any official request (audit report, close-up documentation, other). For audit reports not containing critical finding, Operator shall provide a response within twenty (20) business days.

9.3.4. For SOX regulated systems, in addition, each calendar year, Operator shall engage at its cost and expense a nationally-recognized audit firm acceptable by the Responsible Party to conduct an audit which shall cover, at a minimum, Operator’ quality policies and procedures and controls. Upon the Responsible Party's request, Operator shall provide the Responsible Party with a copy of such report such as a SSAE-16 SOC 2 Type II.

9.4. Operator oversight of subcontractors

Operator shall ensure control over the delegated tasks to its authorized subcontractors on an ongoing basis. In any case, Operator remains liable towards the Responsible Party for its information security and quality obligations even if some of them are fully or partially delegated.

10. DISASTER RECOVERY AND BUSINESS CONTINUITY

10.1. Operator shall notify the Responsible Party in a timely manner when Services are scheduled to be unavailable due to non-emergency maintenance or enhancements.

10.2. Operator shall be responsible for providing and testing contingency/continuity / Disaster recovery strategy to ensure Services to the Responsible Party if Operator experiences or suffers a disaster. Operator shall make associated testing report available to Responsible Party on request.

10.3. Operator shall maintain its capability to resume provisions of the Services in case of disaster and to bring an alternative arrangement into use for maintaining Responsible Party access to the Services

10.4. In the case of unscheduled unavailability, Operator shall inform and cooperate with the Responsible Party regarding the impacts on Services being unavailable (including causes, effect on Services, and estimated duration).

11. QUALITY RESPONSIBILITIES AND OBLIGATIONS (APPLICABLE FOR GXP AND/OR SOX REGULATED COMPUTERIZED SYSTEMS)

11.1. Roles and responsibilities

Operator shall communicate in writing to the Responsible Party the list of Staff involved in communication interfaces for quality purpose and shall keep it current.

11.2. Obligations

11.2.1. Operator shall provide Services to the Responsible Party in conformance with (i) GxP requirements (ii) the annex 11 volume 4 of the European Good Manufacturing Practice on Computerized Systems (ii) the chapter 21 CFR Part 11 of the Food and Drug Administration on Electronic Records & Electronic Signatures.

11.2.2. Operator shall take all reasonable steps to ensure that Services provided to the Responsible Party have been developed and validated for its intended use and in accordance with an appropriate quality management system.

11.2.3. Operator shall provide when requested by the Responsible Party, objective evidence to demonstrate compliance with the clauses documented within this document.

11.2.4. Operator shall ensure that all Staff involved in the provision of computerized system and / or Services per the Agreement have been trained according to their job duties.

11.2.5. Operator shall provide evidence of education and training on any relevant regulations, standards, and processes as applicable for those Staff involved in Services provided.

11.2.6. Operator shall ensure that Audit Trails are enabled properly for all applicable GxP records (i.e. user access records, master data, dynamic data etc.) and as per agreement with the Responsible Party.

11.2.7. Operator shall maintain, monitor, and as necessary improve and update a comprehensive, written “Quality Assurance Plan”. The Quality Assurance Plan shall describe how Operator will implement, when applicable, each quality measure listed in this document. The Quality Assurance Plan shall be validated by the Responsible Party prior to the start of the performance of the Services.

11.3. Incident impacting Responsible Party Data Integrity or compliance (does not apply to Security and Personal Data related incidents)

11.3.1. Operator shall detect and record any Incident affecting Responsible Party Data Integrity, or impacting compliance, functionality or availability of Services provided. Operator must have an Incident process in place.

11.3.2. Operator shall ensure an efficient and prompt handling of Incident affecting Responsible Party Data Integrity, or impacting compliance, functionality or availability of Services and shall make the report to the Responsible Party upon discovery of critical Incident within reasonable timeframe.

11.3.3. Operator shall implement correction and/or corrective and preventive action plans to remedy the Incident and prevent further similar event.

11.4. Regulatory inspections & inquiries and the Responsible Party internal audit

11.4.1. In the event either Party is notified of any regulatory inspection, inquiry or internal Responsible Party audit that relates directly to Services provided by Operator, the Party shall promptly inform the other Party of any such regulatory inspection, audit or inquiry.

11.4.2. In this case, Operator shall permit a designee from the Responsible Party to be present at the Operator option.

11.4.3. Operator agrees that, during any such regulatory inspection, it shall permit any inspection of its processes, documents and premises by or on behalf of regulatory authorities and shall have the resources available to address the requests of any inspectors. Documents maintained by the Operator must be "inspection-ready".

11.4.4. Operator agrees that during the Responsible Party internal audit, Operator shall provide the resources available to address the requests of internal Responsible Party auditors.

11.4.5. The Operator shall not charge the Responsible Party for its time associated with assisting the inspectors / auditors during such event.