Exhibit 1

General Terms and Conditions - Joint Controllership Agreement

PARTIES

JANSSEN PHARMACEUTICA NV (address**)**	JANSSEN PHARMACEUTICA NV , B-2340 Beerse, Belgium, Turnhoutseweg 30
Vendor Name & Addressnsert	Insert Vendor name
MARGO ID	Insert
Date Project initiated	Insert
MSA Start date	Insert
Governing Law and Jurisdiction Country	Insert

JOINT CONTROLLERSHIP AGREEMENT

The Parties have entered into a Project Specification. This Joint Controllership Agreement ("**Joint Controllership Agreement**") forms part of the aforementioned Agreement between the Parties.

As the Parties shall jointly determine the purpose of the data processing operations set out in **Appendix A** and the resources used therefore, Parties shall thus be Joint Controllers within the meaning of Article 26 in Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**GDPR**") and Applicable Data Protection Laws.

This Joint Controllership Agreement regulates the joint Processing, i.e., mutual relations between the Parties as regards to the joint control of Personal Data, and in particular determines the Joint Controller's responsibilities for compliance with the obligations under Applicable Data Protection Law in a transparent manner.

The details of such joint Processing and in particular the Processing activities for which they are jointly responsible, their purposes, the Data Subjects and categories of Personal Data, and the duration of the Processing are described in **Appendix A**.

The Parties accept and agree that such joint controllership is limited to the Processing described in **Appendix A** and does not extend to any Processing undertaken by either Party outside the scope of the Agreement.

Insofar as the Parties process Personal Data in the context of their cooperation outside of the Processing activities described in **Appendix A** they shall each act as sole responsible Data Controller for such Processing activity(ies), including the Personal Data pertaining to each Joint Controller's respective personnel exchanged between the Parties for the administrative management of this contractual relationship and for which each Party remains an independent Controller.

1. DEFINITIONS AND QUALIFICATIONS

1.1 The Parties agree that the terms "**Personal Data Breach**", "**Data Subject**", "**Personal Data**", "**Controller**", "**Supervisory Authority**", "**Data Protection Impact Assessment**" and "**Third Party(ies)**"

shall have the meaning assigned to them as contemplated by Applicable Data Protection Laws and in this Joint Controllership Agreement.

1.2 "**Applicable Data Protection Law**" means the Personal Data protection laws, rules and regulations applicable in the country where the Controller(s)/Joint Controllers is(are) established, or which shall apply based on the terms defining their scope of applicability.

1.3 "**Joint Controller**" means a Controller which, jointly with one or several other Controller(s), determines the purpose(s) and means of the Processing. The Partners are Joint Controllers of the Processing, the purpose which is detailed in **Appendix A**.

1.4 "**Processor**" means any natural or legal person Processing Personal Data, with the approval of one or more Joint Controllers, on behalf of either or both of the Joint Controllers.

1.5 "**Process**", "**Processed**" and "**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automatic means, including the collection, creation, possession, use, disclosure, transfer, storage, deletion, combination, access or other use of Personal Data as contemplated by Applicable Data Protection Law and as described in **Appendix A**, and excluding the Personal Data pertaining to each Joint Controller's respective personnel exchanged between the Parties for the administrative management of this contractual relationship and for which each Party remains an independent Controller.

1.6 "**Sub-processor**" means any natural or legal person engaged by a Processor for the performance of all or part of the Processing operated on behalf of either of the Joint Controllers.

2. OBLIGATIONS AS JOINT CONTROLLERS

2.1 The Parties expressly agree that, for the purposes of the Agreement], they jointly need to Process Personal Data as described in **Appendix A** below, which defines the purpose, scope, modalities and means of the Processing, as well as categories of Data Subjects concerned by the Processing.

2.2 Accordingly, the Parties declare that they shall process the Personal Data in a proper, lawful, and transparent manner as joint controllers, in accordance with Applicable Data Protection Law and this Joint Controllership Agreement.

2.3 In this respect, and subject to the allocation of responsibilities set out in section 2 of Appendix A, each Joint Controller shall:

- exercise due diligence in processing Personal Data, and process Personal Data pursuant to the Joint Controllership Agreement, the Applicable Data Protection Law and/or other provisions of Applicable Data Protection Law, including the appropriate provisions of each Controller's national laws and/or regulations, in such a way as to not expose the other Joint Controller to any violation of Applicable Data Protection Law.

- prevent, remedy and minimize the occurrence of any potential violation of Applicable Data Protection Law with respect to the Processing of Personal Data, and demonstrate compliance with Applicable Data Protection Law by maintaining all relevant documentation to be able to demonstrate its compliance with Applicable Data Protection Law and with the provisions of this Joint Controllership Agreement; and ensuring that it implements the necessary measures to comply with Applicable Data Protection Law in its role as Joint Controller, notably but not limited to the obligation to maintain a record of the Processing in its own register of processing activities; or to conduct a Data Protection Impact Assessment when required by Applicable Data Protection Law.

- agree on a contact point for Data Subjects, that will address inquiries, requests or demands from data subjects and other individuals, national or European Union public administrations, including relevant Supervisory Authorities and courts, as well as any controls or inspections by such authorities in connection with the joint controllership of Personal Data. The party acting as contact point will keep the other party informed at all times and request its collaboration, as required.

- timely inform the other Party(ies), as the case may be, of its inability to comply with its obligations under Applicable Data Protection Law, this Joint Controllership Agreement for whatever reason, or of its Processors' inability to comply with its obligations as Processor in the context of this Joint Controllership Agreement; in such a case, the other Party(ies) shall be entitled to terminate the Joint Controllership Agreement at its sole discretion without incurring any liability.

- timely inform the other Party(ies) if it (i) has reason to believe that all or part of the Processing infringes Applicable Data Protection Law or any relevant applicable law; and, in addition, timely inform the other Party(ies) of (ii) any change in the conditions of performance of its activities which may modify or otherwise impact in any way the specifications of the Processing as described in **Appendix A.** Any such change as well as any new Processing may only be implemented or carried out in compliance with this Joint Controllership Agreement.

- process and retain the Personal Data only for the term(s) of retention as set out in **Appendix A** and in any event for no longer than any statutory or professional retention periods under any Applicable Data Protection Law or other mandatory laws or regulations.

- process the Personal Data only for the purpose(s) set forth in **Appendix A** and in accordance with the Agreement, including this Joint Controllership Agreement and commit to processing the Personal Data exclusively for the purpose for which the Personal Data were collected.

- process the Personal Data for any other purpose(s) only if such further Processing complies with Applicable Data Protection Law and the other Party has agreed with such further Processing; in such case, the concerned Parties shall, as independent Controllers, be solely responsible for the compliance of such Processing with Applicable Data Protection Law, including, notably, to ensure that it has a legal ground to implement such Processing. Where Personal Data Processed are of a less sensitive category, the Parties may agree that any use beyond the purposes for which they were originally Processed shall be subject to notification to the other Party in due time and the absence of an objection.

- be entitled to entrust Processors with the processing of Personal Data, provided that such processing is done on a lawful basis and in compliance with applicable regulatory and legal requirements. Each Party will select Processors and Sub-processors in accordance with their expertise in such Processing activity and their ability to implement appropriate technical and organizational measures for the protection of the personal data. The Parties have identified approved Processors and Sub-processors in **Appendix A** of this Joint Controllership Agreement.

- keep and provide to the relevant Party, upon the latter's written request, all documents or evidence necessary to establish its compliance with this Joint Controllership Agreement and with the Applicable Data Protection Law relating to the shared Processing.

3. NON-DISCLOSURE AND CONFIDENTIALITY

3.1 All Personal Data are considered confidential information and must therefore be treated as confidential information. The Parties shall impose this duty of confidentiality on all the natural persons and legal entities they engage to process Personal Data, including but not limited to employees, data Processors, Third Parties and other recipients of Personal Data.

3.2 The Parties shall keep all Personal Data secret and shall not disclose the Personal Data to internal or external parties in any way whatsoever, except in cases where:

- disclosure and/or transmission of the Personal Data is necessary for the performance of the Agreement;
- the Parties are required to disclose, transmit and/or transfer the Personal Data due to mandatory legal provisions or a court order issued by a competent court or on the orders of some other government agency having authority over the Parties, although the Parties shall first notify the other Parties of this requirement;
- the Personal Data are disclosed and/or transmitted with the other Parties' prior Written consent; or
- one or both of the parties are subject to a legal obligation which requires the disclosure of such data. The Parties shall communicate these obligations in advance to the other party.

4. LIABILITY

4.1 The liability of the Parties is governed by the legal regulations, in particular Article 82 of the GDPR and relevant corresponding articles in Applicable Data Protection Laws with regard to the processing activities as described in **Appendix A**.

4.2 Each Party indemnifies the other Party against all damages resulting from its own infringement of its obligations under this Joint Controllership Agreement and/or Applicable Data Protection Laws. Each Party therefore commits to hold the other Party harmless in respect of of any claim or action by any third party as well as any sanction by any jurisdiction or authority grounded on or resulting from its own infringement of its obligations under this Joint Controllership Agreement and/or Applicable Data Protection Laws.

5. TERM AND TERMINATION

5.1 This Joint Controllership Agreement shall remain in force until complete deletion or return by each Party of the Personal Data, which will not take place in any event before the termination of the Agreement.

5.2 **Termination for breach.** In the event of a material breach of the terms of this Joint Controllership Agreement and caused by a party's errors or omissions, the other party may terminate the Joint Controllership Agreement and the Agreement with immediate effect.

5.3 This Joint Controllership Agreement cannot be terminated independently from the Agreement. If the Agreement is terminated, the Joint Controllership Agreement shall also be terminated.

5.4 Upon termination or expiration of the Agreement and/or the statutory retention periods has/have expired, the Parties shall immediately cease handling Personal Data and will ensure jointly that the Personal Data are destroyed except as otherwise required by Applicable Data Protection Law.

5.5 This Joint Controllership Agreement can only be amended by the Parties following a consultation of all participating Parties, and provided that all participating Parties have agreed to the proposed amendment. If Applicable Data Protection Law and regulations are amended, the Parties shall seek to amend this Joint Controllership Agreement accordingly.

6. MISCELLANEOUS

6.1 **Governing Law and Jurisdiction.** This Joint Controllership Agreement and and its performance are governed by the law of **Named Country** (see table above). If any disputes relating to the Agreement should arise between the Parties, they must be brought before the court that is competent to rule on them pursuant to the Agreement.

6.2 **Invalidation.** In the event that one or more provisions of this Joint Controllership Agreement should prove to be legally invalid, the validity of the remaining provisions of this Joint Controllership Agreement shall be unaffected. In such cases, the Parties shall consult each other on the provisions that are not legally valid so as to be able to come to an agreement that is legally valid and obeys the letter and spirit of the provision that requires amendment.

6.3 **International data transfer**

The Parties do not anticipate any transfers of Personal Data outside UK and EEA.

6.4 **Contact persons and data protection officers**

JANSSEN (J&J) CONTACT PERSON (PROJECT OWNER) NAME	Insert
JANSSEN (J&J) CONTACT PERSON (PROJECT OWNER) E-MAIL	Insert
JANSSEN (J&J) DPO CONTACT ADDRESS	EMEAPRIVACY@ITS.JNJ.COM
VENDOR CONTACT PERSON (PROJECT LEAD) NAME	Insert
VENDOR CONTACT PERSON (PROJECT LEAD) E-MAIL ADDRESS	Insert
VENDOR DPO CONTACT ADDRESS	XXXX (ASK THE VENDOR TO INSERT)

If contact persons change or are prevented from acting as contact persons, the other Party will be informed without undue delay and in writing of the successors or replacement representatives.

The parties have caused this Joint Controllership Agreement to be executed by their duly authorized representatives.

Signatures:	**Janssen (J&J)**	**InPharmation**
Signed By		

Name	Insert	Insert
Title	Insert	Insert
Date	XXXXX	XXXXX

APPENDIX A. DESCRIPTION OF THE PROCESSING AND ALLOCATION OF RESPONSIBILITIES

1. DESCRIPTION OF THE PROCESSING OF PERSONAL DATA

In addition to the Joint Controllership Agreement, this **Appendix A** describes the particulars and details of the Processing:

1.1 Objective of the Study	Insert from initiation template	

1.2 Reasons for the need of JCA: Tick all boxes that applies in 1.2

Activities Carried out by J&J	
Sharing target list by J&J	☐
Conducting research with Patients or Caregivers	☐
Listening, Viewing by J&J members or access to personal data	☐
Input int Market research Design	☒
Activities Carried out by Vendor	***Insert***
Using target list to recruit from	☐
Anonymize Personal Data contained in the results of the study prior to sharing the results with Janssen/ J&J.	☒

1.3 Legal basis for the Processing

☐ Consent
☐ Contractual obligation
☐ Legal Obligation
☐ Vital interests
☐ Public interests
☐ Legitimate interests

1.4 Nature of the Processing

The Processing of the Personal Data includes the following operations:

Janssen	**Agency**
☐ Collection	☒ Collection

☐ Consultation	☒ Consultation
☐ Recording	☒ Recording
☐ Use	☒ Use
☐ Organization	☒ Organization
☐ Disclosure	☒ Disclosure
☐ Structuring	☒ Structuring
☒ Making available	☒ Making available
☐ Storage	☒ Storage
☐ Alignment / Combination / Matching	☒ Alignment / Combination / Matching
☐ Adaptation	☐ Adaptation
☐ Restriction of use or access	☒ Restriction of use or access
☐ Retrieval	☐ Retrieval
☐ Erasure or destruction	☒ Erasure or destruction
☒ Remote access	☒ Remote access
☐ Media handling (e.g. transportation of media containing Personal Data)	☒ Media handling (e.g. transportation of media containing Personal Data)
☒ Other. Viewing of live interviews	☐ Other. Please Specify
☐ No access to Personal Data – Aggregated data only	☐ No access to Personal Data – Aggregated data only

1.5 Categories of Data Subjects

The Personal Data processed relates to the following categories of Data Subjects:

☐ Employees
☐ Patients or their relatives (e.g., participants to a clinical study, users of an application, persons we are in contact with regarding our products)
☒ Healthcare professionals (*general practitioners, key opinion leaders, nurses, pharmacists, dentists, etc.*)
☐ External contractors
☐ Other. Please specify:

1.6 Type of Personal Data

The Personal Data Processed concerns the following types of data:

☐ Network ID or connection data *(ID, password, etc.)*
☒ Identity information (*name, email, address, phone number, photo, etc.*)
☐ Personal life data (*marital status, children, etc.*)
☒ Professional life data (*qualifications, skills, position, professional goals, etc.*)
☒ Economical/financial information (*bank account details, income, etc.*)
☐ Location data (*GPS, etc.*)
☐ Sensitive data (*health, racial/ethnic origins, religious or philosophical beliefs, political opinions, trade-union membership, sex life, etc.*). If sensitive data are Processed, specify which category (select all applicable categories):

☐ *Data relating to health*
☐ *Racial/ethnic origin*
☐ *Religious or philosophical beliefs or political opinions,*
☐ *Trade-union membership,*
☐ *Sex life*
☐ *Biometric data (fingerprints, iris scan, hand geometry, DNA, etc.)*
☐ *Genetic data*
☐ *Social security number*
☐ *Other. Please specify:* _____

1.7 Terms of retention of the categories of Personal Data

Retention period for the Processing activity for the Personal Data, or the criteria used to establish the retention period (describe retention period for each category of Personal Data, as applicable)
Personal data processed as part of this study will be deleted after XXXX. (Ask Vendor to enter)

1.8 Categories of personnel having access to Personal Data

Party	Categories of Party's employees (function roles/function groups) who perform Processing operations	(Category of) Personal Data processed by employees	Type of Data Processing operation
Insert	XXX	XXX	Collection, recording, Use, Organization, Disclosure, Structuring, Making available, Storage, Restriction of use or access, Erasure or destruction, Remote access

1.9 Approved Data Processors

The parties have agreed that the following data processors may be used by the respective parties under the Agreement:

Party	Processors engaged by Party	Country where Personal Data will be Processed	Location of the Processor	Engaged by	Data Processing Agreement	Authorised by other Parties
XXX (if Applicable Ask Vendor to enter)						

2. ALLOCATION OF RESPONSIBILITIES OF THE JOINT CONTROLLERS

	Janssen	Agency
INFORMATION OF DATA SUBJECTS		
Provide all Data Subjects with a complete, transparent, intelligible, accurate and specific information notice in relation to the Processing, containing all mandatory information required under Applicable Data Protection Law, and in particular, the identity of the Joint Controllers, on which additional information might be provided on potential further use of Personal Data (if existing/applicable). Ensure that such information notice is communicated in advance to the other Party(ies) for its comments and observations.	☐	☒
DATA ACCURACY AND RELEVANCE		
Ensure that the Personal Data collected as part of the Data Processing are accurate, relevant and kept up-to-date.	☒	☒
CONSENT		
Obtain, where applicable, the Data Subjects' free, specific, informed unambiguous consent to the Processing in accordance with Applicable Data Protection Law, (ii) retain evidence of the Data Subject's consent to the Processing through the proper retention period, (iii) ensure Data Subjects can exercise their right to withdraw their consent at any time. Ensure that the form used to collect consent is communicated in advance to the Other Parties for their comments and observations.	☐	☒
DATA SUBJECT RIGHTS		
Ensure that Data Subjects can exercise effectively their rights, as granted by Applicable Data Protection Law, regarding the Processing.	☐	☒
Implement, where applicable, adequate technical and organizational measures designed to ensure that the Party can address all requests from Data Subjects for the exercise of the rights as granted by Applicable Data Protection Law regarding the Processing.	☐	☒
Cooperate with the Party responsible for addressing the requests from Data Subjects and provide assistance regarding all elements falling in its purview in order to permit this Party to implement relevant measures.	☒	☒

Act as single point of contact for Data Subjects with respect to the Processing, providing adequate mechanisms concerning any relevant request regarding privacy rights, or any issue related to the Agency's privacy policy and distribution of obligations and responsibilities.	☐	☒
Provide a channel for Data Subjects to exercise their privacy rights, as provided under Applicable Data Protection Law.	☐	☒
Timely communicate with the other Party / refer any query.	☒	☒
Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, assisting the other Party where necessary to comply with its obligations.	☒	☒
SECURITY MEASURES		
Implement appropriate technical and organizational security measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction or damage, taking into consideration the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, and the risks for the Data Subjects.	☐	☒
Where applicable, proceed to the full and irreversible anonymization of the Personal Data, and warrant that such anonymization process complies with Applicable Data Protection Laws.	☐	☒
PRIVACY BY DESIGN		
Determine and implement data protection principles from the design stage and by default, in accordance with Art. 25 of the GDPR.	☒	☒
DISCLOSURE OF PERSONAL DATA		
Disclose the Personal Data only to the categories of recipients listed in Appendix A. Restrict access to Personal Data only to persons who need the access to Personal Data for the purposes of the Agreement, and to that which is minimally necessary and provide those persons with specific authorizations, offer relevant training on personal data protection and ensure confidentiality of Personal Data processed thereby, both during and after their employment or other cooperation with a Joint Controller.	☒	☒
Notify the other Party(ies) if new recipients of the Personal Data are appointed by one of the Parties, in order to allow the other Party(ies) to reasonably object to such disclosure.	☒	☒

PERSONAL DATA BREACH

Each Party shall be separately responsible for reporting a Personal Data Breach to the Supervisory Authority and/or affected Data Subjects if a Personal Data Breach occurred under its responsibility. Both Parties will reasonably assist each other and cooperate (1) to investigate any such Personal Data Breach, (2) jointly decide whether a notification to any Supervisory Authority, individual or any third party shall be performed, and (3), as jointly determined, to notify affected individuals, regulatory bodies, or credit reporting agencies with respect to such Data Breach.

Accordingly each Party shall notify the other Party in writing as soon as possible without undue delay (and in any event within 48 hours) whenever a Party reasonably believes that there has been a Personal Data Breach. Such notice will provide detailed information regarding the Personal Data Breach, including its nature and scope; actual or potential cause; any reports to law enforcement; and, measures being taken to investigate, correct, mitigate, and prevent future Personal Data Breaches.

Each Party is separately responsible for recording and/or documenting Personal Data Breaches in their own register or systems.

If any costs are incurred in the attempt to resolve the Personal Data Breach and implementing mitigating and remediating controls to prevent recurrence in the future, said costs shall be borne by the Party who had possession or control of the data within its operating range.

Comply with Applicable Data Protection Law in the event of a Personal Data Breach arising during the Processing, and in particular, (i) inform the other Party(ies) about such Personal Data Breach within forty-eight (48) hours of becoming aware of it; (ii) take such actions as may be necessary or reasonably expected in the state of the art to minimize the effects of any Personal Data Breach; and (iii) take all actions as may be required by Applicable Data Protection Law, particularly regarding communication to Data Subjects and notification of Supervisory Authorities.	☒	☒

DATA PROTECTION IMPACT ASSESSEMENT		
Determine whether the Processing requires a data protection impact assessment in light of Applicable Data Protection Law and, as applicable, carry out such assessment.	☒	☒
Timely submit the outcome of such data protection impact assessment and its content to the other Party(ies) for its comments and observations.	☐	☐
Consult the other Party(ies) on the communication to be made to applicable Supervisory Authority.	☒	☐

RELATIONS WITH SUPERVISORY AUTHORITY		
Determine whether the data Processing requires the consultation or prior approval of the competent Supervisory Authority.	☒	☒
Be the appointed Party to answer any queries or requests for information by competent Supervisory Authorities.	☐	☒
Promptly inform and consult with the other Party(ies) in the event of queries, requests for information or investigations from competent Supervisory Authorities, and seek prior advice from the other Party(ies) before any filing, declaration, statement or communication to any Supervisory Authority or any other intended third-party recipient.	☒	☒
Notify the other Party(ies) (i) in case of any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless otherwise legally prohibited and (ii) in case of any notification received from a Supervisory Authority alleging infringement of the Applicable Data Protection Law in the course of the Processing, or of the exercise by a Supervisory Authority of its corrective powers provided by the Applicable Data Protection Law where such exercise is related to, or has an effect upon, the Processing.	☒	☒
DATA TRANSFERS SAFEGUARDS		
Ensure, where applicable, that all transfers of Personal Data in the context of the Processing outside of the region where it is originally collected or hosted, are governed by relevant safeguards to maintain an adequate protection of Personal Data and obtain, as applicable, any relevant consents, authorizations or permits from Data Subjects or competent Supervisory Authorities.	☐	☒
PROCESSING/ SUBPROCESSING AND SUBCONTRACTING OTHER DATA CONTROLLERS		
Ensure that all Processors and Sub-processors selected for the purpose of the Processing provide sufficient guarantees and implement appropriate technical and organisational measures to comply with its obligations as Processor as set forth by Applicable Data Protection Laws and meet the requirements of this exhibit, throughout the entire term of the Agreement.	☐	☒
Ensure that all Sub-contractors in a role of Data Controllers (Joint or Sole) engaged into the Processing of the Personal Data are legally bound by the same obligations as the subcontracting Party is bound by under this Joint Controllership Agreement to the extent necessary to comply with Applicable Data Protection Law and this Joint Controllership Agreement.	☐	☒

RECORDS OF PROCESSSING ACTIVITIES		
Maintain its own records of processing activities, in accordance to Applicable Data Protection Law.	☒	☒
DELETION OF PERSONAL DATA		
Delete or return all and any Personal Data for the purpose of performance of the Agreement, without prejudice to the retention of data as required by applicable law or for the establishment, exercise of defence of actual or potential legal claims, during the applicable statutory limitation periods.	☒	☒
ACT AS CONTACT POINT FOR THE DATA SUBJECTS		
Address inquiries, requests or demands from data subjects and other individuals, national or European Union public administrations, including relevant supervisory authorities and courts, as well as any controls or inspections by such authorities in connection with the joint controllership of Personal Data.	☐	☒
Keep the other party always informed and require its collaboration, as required.	☒	☒

APPENDIX B. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. Each Party shall maintain an information security program that encompasses administrative, technical, and physical safeguards that meet or exceed the requirements specified in Applicable Data Protection Laws and applicable industry standards to protect against threats to the unauthorized or accidental destruction, loss, alteration, or use of Personal Data, and/or unauthorized disclosure or access to Personal Data.

2. Party personnel who are provided ongoing access to facilities and/or network and computing resources shall abide by all applicable Acceptable Use policies and complete information security training. For such personnel, each Party shall conduct background checks and/or other investigations deemed necessary, as appropriate and permitted by applicable law. Personnel access or connectivity may be terminated at any time upon violation of policies and/or misuse or abuse of privileges.

3. If either Party discovers or is notified of a breach or potential breach of security relating to Personal Data, or that would otherwise interrupt or degrade business operations of the Parties, a Party shall: (a) notify the other Party within 48 hours of such breach or potential breach; and (b) (i) promptly investigate and remediate the effects of the breach or potential breach, and (ii) provide the other Party with satisfactory assurance that such breach or potential breach will not reoccur.

4. No Personal Data shall be sold, assigned, leased or otherwise disposed of to a third party, or commercially exploited, by or on behalf of either Party or its personnel without express written

consent. The Parties shall not collect, share, disclose or use any Personal Data except as necessary to perform the services described in the Agreement. Furthermore, each Party represents and acknowledges that it does not receive, nor is it providing, any such Personal Data in consideration for the provision of the services or otherwise.