# SUB-OPERATOR AGREEMENT

between

***DIVISION NAME TO BE INSERTED***

(Registration number: ______________)

(Hereinafter referred to as **“the Company”)**

and

***OPERATOR NAME TO BE INSERTED***

(Registration number: ……………………)

(Hereinafter referred to as the **“Operator”)**

and

***SUB-OPERATOR NAME TO BE INSERTED***

(Registration number: ……………………)

(Hereinafter referred to as the **“Sub-Operator”)**

## 1. INTRODUCTION

1.1 In terms of section 20 of POPIA, where a Responsible Party asks other parties (hereinafter referred to as an "Operator") to process Personal Information or further process Personal Information belonging to its Data Subjects on its behalf, whether in South Africa or outside South Africa**,** then any such processing must be subject to a written agreement concluded between the parties which contractually obliges the Operator or Sub-Operator to:

1.1.1 comply with the provisions of POPIA and the POPIA processing conditions when processing such Personal Information on behalf of the Company;

1.1.2 only process the Personal Information in accordance with the mandate or written instruction received from the Responsible Party and/or in accordance with the provisions set out under "Annexure A", "Annexure B" and "Annexure C";

1.1.3 keep all the Personal Information on behalf of the Responsible Party and/or belonging to the Responsible Party's Data Subjects, confidential;

1.1.4 put measures in place in order to keep all such Personal Information held by the Operator, and processed on behalf of the Responsible Party, confidential, safe and secure from misuse, abuse and/or unauthorised use or access.

1.2 Furthermore, where any Operator is desirous of appointing a Sub-Operator to process any Personal Information that belongs to the Responsible Party's Data Subjects on its behalf, any such processing must be subject to a written agreement concluded between the Responsible Party, the Operator and the Sub-Operator that contractually obliges the Sub-Operator to comply with the requirements set out under clause 1.1.1 - 1.1.4 above.

1.3 The Operator will provide the Sub-Operator with certain Personal Information that pertains to certain of the Company's Data Subjects, for processing on its behalf, and the Company has agreed that this may take place subject to the terms and conditions set out under this Sub-Operator Agreement.

## 2. DEFINITIONS

2.1 The parties must take note of the following definitions, which will be used throughout this Sub-Operator Agreement, unless the context indicates a contrary meaning:

2.1.1 "**Company**" means Libstar Holdings Limited, a limited liability company incorporated in South Africa with registration number 014/032444/06 and its operating subsidiaries (including Glenmor Soap (Pty) Ltd – registration number 2011/149475/07 and Libstar Operations (Pty) Ltd – registration number 2014/062496/07), as defined by the Companies Act 71 of 2008 as amended; who has mandated the Operator and / or Sub-Operator to process certain Personal Information belonging to Data Subjects on its behalf, per the terms of this Agreement / Addendum and where applicable any detailed mandate which is attached hereto marked "Annexure A";

2.1.2 **"Data Subject(s)"** means the person(s) who own(s) the Personal Information that is to be processed by the Sub-Operator on behalf of the Operator in terms of this Sub-Operator Agreement;

2.1.3 **"Operator"** means the person who has been mandated by the Company in terms of the Agreement / Addendum to processes Personal Information belonging to certain Data Subject(s) on its behalf;

2.1.4 **“Operator Agreement”** means the Operator Agreement concluded between the Company and the Operator;

2.1.5 **"person"** means an identifiable, living, natural person, or an identifiable, existing juristic person;

2.1.6 **"Personal Information"** means personal information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:

- **in the case of an individual:**
  - name, address, contact details, date of birth, place of birth, identity number, passport number, bank details, details about your employment, tax number and financial information;
  - vehicle registration;
  - dietary preferences;
  - financial history;
  - information about next of kin and/or dependants;
  - information relating to education or employment history; and

  - **Special Personal Information** including race, gender, pregnancy, national, ethnic or social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

- **in the case of a juristic person:**
  - name, address, contact details, registration details, financials and related history, B-BBEE scorecard, registered address, description of operations, bank details, details about employees, business partners, customers, tax number, VAT number and other financial information; and

- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

- the views or opinions of another individual about the person; and

- the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.1.7 **"Process or processing"** means any operation or activity or any set of operations, whether by manual or automatic means, performed by the Sub-Operator concerning a Data Subject’s Personal Information, including:

(a) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.1.8 **"record"** means any recorded information:

(a) regardless of form or medium, including any of the following:

(i) writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a Responsible Party;

(c) whether or not it was created by a Responsible Party; and

(d) regardless of when it came into existence.

2.1.9 **"Sub-Operator"** means ______________________________________________(*insert individual or legal entity name)*, who has been appointed by the Operator, on approval by the Company, to process certain Personal Information on its behalf in terms of this Sub-Operator Agreement;

2.1.10 **"Sub-Operator Agreement"** means this Sub-Operator Agreement.

## 3. MANDATE TO PROCESS

The Operator hereby grants to the Sub-Operator a mandate to process certain Personal Information on its behalf, per the mandate set out under "Annexure A" attached hereto. The parties agree that this sub-processing may only take place on the terms set out under this Sub-Operating Agreement.

## 4. OBLIGATIONS OF THE SUB-OPERATOR

4.1 The Sub-Operator expressly warrants and undertakes that it will:

4.1.1 process the Personal Information strictly in accordance with its mandate set out under the Sub-Operator Agreement read together with “Annexure A”, “Annexure B” and “Annexure C” and any specific instructions provided to it by the Company or the Operator from time to time;

4.1.2 not use the Personal Information for any other purpose, save for the purpose set out under this Sub-Operator Agreement and “Annexure A”;

4.1.3 only disclose, transfer and/or handover the Personal Information to person(s) identified under Annexure A;

4.1.4 save for the provisions recorded under clause 4.1.3, treat the Personal Information as confidential and not disclose the Personal Information to any other person unless required by law. The disclosure, transfer or handover of Personal Information should only be done after the Sub-Operator has provided the Company with adequate warning of this requirement and the related details thereof. Details provided to the Company should include the identity of the person or legal entity who is to receive the Personal Information, the reason for the disclosure and confirmation that the person or legal entity to whom the Personal Information is to be disclosed to, has signed the POPIA onwards transmission notice attached hereto marked “Annexure B”;

4.1.5 has, and will continue to have in place, appropriate technical and organisational measures to protect and safeguard the Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and which, in addition, provides a level of security appropriate to the risk represented by the processing and the nature of the Personal Information to be protected The safeguards must comply with the requirements set out under POPIA and be in line with the requirements described under the attached “Annexure C”;

4.1.6 notify the Operator and the Company immediately where it has reasonable grounds to believe that the Personal Information that has been provided to it, including any Personal Information which it has processed, has been lost, destroyed, or accessed or acquired by any unauthorised person;

4.1.7 process the Personal Information strictly in accordance with POPIA and the POPIA processing conditions;

4.1.8 not use the Personal Information for any direct marketing or advertising, research or statistical purposes, unless expressly authorised to do so as described under “Annexure A”. When conducting such activity, the Sub-Operator must ensure that this is done strictly in compliance with the requirements of POPIA and its regulations especially those applicable to direct marketing detailed under Section 69 of the Act;

4.1.9 not treat the Personal Information as its own, it expressly acknowledges that it has been tasked with processing the Personal Information in its capacity as the Company’s Operator / Sub-Operator and agent, and that ownership of all the records recording the Personal Information and any records comprising such Personal Information pertaining to the Data Subject, will always remain with the Company;

4.1.10 not sell, alienate or otherwise part with the Personal Information or any of the records recording the Personal Information;

4.1.11 where it is allowed to transfer the Personal Information onwards to any third party, ensure that such party concludes a written onwards transfer agreement (Annexure B) with it to ensure POPIA Compliance.

4.1.12 ensure that any person acting under the authority of the Sub-Operator, including any employee or Sub-Operator, shall be obligated to process the Personal Information only on instructions from the Sub-Operator and strictly in accordance with this Sub-Operator Agreement.

4.2 The Sub-Operator warrants that it has the legal authority to give the above-mentioned warranties and fulfil the undertakings set out in this Sub-Operator Agreement.

4.3 The Company in order to ascertain compliance with the warranties and undertakings recorded under this Agreement, will have the right, on reasonable notice and during regular business hours, to view and/or audit, either by itself or through an independent agent, the Operator's facilities, files, and any other data processing documentation required for the audit and/or independent or impartial inspection. The Sub-Operator undertakes to provide all necessary assistance that may be required to give effect to this requirement.

## 5. LIABILITY OF THE OPERATOR AND THIRD-PARTY RIGHTS

5.1 In the event of the Operator, the Sub-Operator or their respective employees or agents failing to comply with any of the provisions of POPIA or breaching any of the warranties and undertakings recorded under this Agreement / Addendum or the Sub-Operator agreement where applicable, the Operator shall be liable for all and any damages it or the Sub-Operator may have caused in consequence of said breach or non-compliance, including patrimonial, non-patrimonial and punitive damages suffered by the Company and/or the Data Subject(s). The Operator indemnifies and holds the Company including its directors, employees and all and any affected Data Subjects harmless against any such loss, damage, action or claim which may be brought by whomsoever against the Company or any of its directors, employees, or Data Subjects, or against any of the Company's affiliated companies, or their directors or employees, and agrees to pay all and any such amounts on demand.

## 6. APPLICABLE LAW

The laws of South Africa shall apply to this Agreement, regardless of where the Personal Information is, will be, or was actually processed.

## 7. TERMINATION

7.1 In the event of:

7.1.1 the Sub-Operator Agreement being terminated for any reason;

7.1.2 the Operator Agreement being terminated for any reason;

7.1.3 the transfer of Personal Information to the Operator being temporarily suspended by the Company for any reason;

7.1.4 the Sub-Operator being in breach of its obligations under the Sub-Operator Agreement or has failed to comply with POPIA or the Information Processing Principles, and has failed when called upon to do so by the Company or the Operator to rectify the breach or area of non-compliance;

7.1.5 the Sub-Operator being in substantial or persistent breach of any warranties or undertakings given by it under the Sub–Operator Agreement, notwithstanding that the Company or the Operator has not given the Sub-Operator notice of such breach;

7.1.6 an application is filed for the placing of the Operator or Sub-Operator under business rescue, under administration, or winding up whether interim or final, which application is not dismissed within the applicable period for such dismissal under applicable law; or any equivalent event in any jurisdiction occurs,

then the Company or the Operator, without prejudice to any other rights, which it may have against the Sub-Operator, shall be entitled to terminate, where applicable the Sub-Operator Agreement, as well as, where applicable, any other Sub-Operator agreement.

7.2 The Parties agree that the termination of the Sub-Operator Agreement at any time, in any circumstances and for any reason, does not exempt them from the rights and obligations set out under this Sub-Operator Agreement with regards to the processing of the Personal Information detailed under “Annexure A”, “Annexure B” and “Annexure C”, read together with the obligations under POPIA.

7.3 In the event of the Sub-Operator Agreement being terminated at any time and for any reason, the Sub-Operator undertakes to:

7.3.1 restore and/or transfer back to the Company all and any Personal Information that has been provided to the Operator for processing, including that held by the Sub-Operator, whether same has been processed or not, and/or which has been processed together with any related documentation and/or information. All aforementioned documentation must, without exception, be returned to the Company within a period of 30 (thirty) days from the date of service of the termination notice.

7.3.2 to confirm in writing simultaneously when the transfer under clause 7.3.1 takes place, that all such Personal Information will be kept confidential as per the provisions of clause 4.1 and that it will not under any circumstances use the aforementioned information for any reason.

8 Notwithstanding termination of the Sub-Operator Agreement and for whatsoever reason, the clauses 4, 5, 6 and 7.2 will survive any such termination.

### 8. GENERAL

8.1 The parties may not modify the provisions of this Sub-Operator Agreement, including the information in “Annexure A”, “Annexure B” or “Annexure C”, unless such variation is reduced to writing and signed by the Parties.

8.2 All notices to be provided in terms of the Agreement, must be sent to the respective Company’s Information Officer or Deputy Information Officer by email at their details recorded on our website.

## Agreement Acceptance and Signatures:

**Sub-Operator**

Name ___________________ Position ___________________

Signature ___________________ Date ___________________

**Company**

Name ___________________ Position ___________________

Signature ___________________ Date ___________________

**ANNEXURE A**

# PROCESSING MANDATE

## 1. DETAILS OF THE COMPANY (RESPONSIBLE PARTY)

[Please insert details of the Responsible party]

## 2. DETAILS OF THE OPERATOR AND SUB-OPERATOR

[Please insert details of the Responsible party]

## 3. DETAILS OF PERSONAL INFORMATION FOR PROCESSING

[Please insert the types of personal information being processed]

## 4. PURPOSE OF PROCESSING

[Please insert the purpose for Processing the Personal Information]

## 5. PROCESSING DETAILS

5.1 DATA SUBJECTS

The Personal Information Processed concern the following Data Subjects:
[Please insert a list of the categories of Data Subjects]

5.2 CATEGORIES OF DATA

The Personal Information transferred concern the following categories of data:
[Please insert a list of the categories of data which will be Processed]

5.3 DETAILS OF THE DATA SUBJECT'S SPECIAL PERSONAL INFORMATION:
[Please insert a list of the Special Personal Information that will be processed. Please note that special Personal Information has to be processed with the data subject's express consent]

**ANNEXURE B**

## ONWARDS TRANSMISSION NOTE

……………………………………………... (Individual or Legal entity name), an Operator acting on behalf of the Company, have agreed to provide you with the following information, which we have been asked to process by the Company on their behalf:

### 1. DETAILS OF THE DATA SUBJECT/S AND OWNER OF THE PERSONAL INFORMATION

………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………

### 2. DETAILS OF THE PERSONAL INFORMATION

………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………

### 3. REASON OR PURPOSE WHY YOU NEED TO PROCESS THE PERSONAL INFORMATION

………………………………………………………………………………………………………………………………………………
………………………………………………………………………………………………………………………………………………

We have obtained permission from the Company and the Data Subject, as indicated below, to provide you with the abovementioned information, which is provided to you on the terms detailed below.

By accepting and receiving the Personal Information you undertake to comply with and abide by these terms:

### 4. CONDITIONS AND TERMS OF USE AND IMPLIED CONSENT TO COMPLY

- You will keep the Personal Information private and confidential;
- You may only use the Personal Information for the purpose described above and for no other purpose;
- You will safeguard the Personal Information;
- You will in particular ensure that the Personal Information is kept safe and secure from unlawful or unauthorised access, and you will ensure that the integrity of the information is not compromised or altered in any manner;
- When using the Personal Information, you will comply with the processing conditions and provisions set out under a law known as the Protection of Personal Information Act, 4 of 2013, (POPIA);
- You agree to indemnify the Data Subject against all and any damages which may be incurred by them as a result of your non-compliance with the above undertakings.

Furthermore, you acknowledge that the Company and/or the Data Subject may institute legal action against you under the provisions recorded under POPIA should you breach the abovementioned terms.

1. Signed by the Company ………………………… Date: …………………………

2. I, the abovementioned data subject, agree to the above onwards transmission of my Personal Information.

Signed by Data Subject ………………………… Date: …………………………

3. Signed by Recipient ………………………… Date: …………………………

**ANNEXURE C**

## TECHNICAL AND ORGANISATIONAL MEASURES FOR DATA PROCESSING TO BE IMPLEMENTED BY THE OPERATOR AND SUB-OPERATOR

### 1. Physical Access Control

Safeguarding admission and access to processing systems against unauthorised parties.

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement:

□ Alarm system

□ Automatic access control system

□ Locking system with code lock

□ Biometric access barriers

□ Light barriers/motion sensors

□ Manual locking system including key regulation

□ Visitor logging

□ Chip cards/transponder locking systems

□ Video monitoring of access doors

□ Safety locks

□ Personnel screening by gatekeeper/reception

□ Careful selection of cleaning and security staff

### 2. Data Access Control / User Control

Prevention of third parties using automatic processing systems with equipment for data transmission.

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum :

□ Authentication with username/password (per valid password regulations)

□ Usage of intrusion detection systems

□ Usage of anti-virus software

□ Usage of a software firewall

□ Creation of user profiles

□ Assignment of user profiles to IT systems

□ Usage of VPN technology

□ Encryption of mobile data storage media

□ Encryption of data storage media in laptops

□ Usage of central smartphone administration software (e.g. for the external erasure of data)

### 3. Data Usage Control / Data Storage Media Control / Memory Control

Ensuring that the parties authorised to use an automated processing system only have access to the Personal Information appropriate for their access authorisation.

Prevention of unauthorised reading, copying, changing or erasure of data storage media (data storage media control).

Prevention of unauthorised entry of Personal Information and unauthorised access to it, changing and deleting saved Personal Information (memory control).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum:

□ Roles and authorisations based on a *"need to know principle"*

□ Number of administrators reduced to only the "essentials"

□ Logging of access to applications, in particular the entry, change and erasure of data

□ Physical erasure of data storage media before reuse

□ Use of shredders or service providers

□ Administration of rights by defined system administrators

□ Password guidelines, including password length and changing passwords

□ Secure storage of data storage media

□ Proper destruction of data storage media

□ Logging of destruction

## 4. Transfer Control/Transportation Control

Ensuring that the confidentiality and integrity of data is protected during the transfer of Personal Information and the transportation of data storage media (e.g. through powerful encryption of data transmissions, closed envelopes used in mailings, encrypted saving on data storage media).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum:

☐ Establishment of dedicated lines or VPN tunnels

☐ Encrypted data transmission on the Internet (such as HTTPS, SFTP, etc.)

☐ E-mail encryption

☐ Documentation of the recipients of data and time frames of planned transmission or agreed erasure deadlines

☐ In case of physical transportation: careful selection of transportation personnel and vehicles

☐ Transmission of data in an anonymised or pseudonymised form

☐ In case of physical transportation: secure containers/packaging

## 5. Entry Control / Transmission Control

Ensuring that it is possible to subsequently review and establish which Personal Information has been entered or changed at what time and by whom in automated processing systems, for instance through logging (entry control).

Depending on the system, ensuring that it is possible to review and determine to which offices or locations Personal Information has been transmitted or provided using equipment for data transmission, or to which offices or locations it could be transmitted (transmission control).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum:

☐ Logging of the entry, change and erasure of data

☐ Traceability of the entry, change and erasure of data through unique usernames (not user groups)

☐ Assignment of rights for the entry, change and erasure of data based on an authorisation concept

☐ Creating an overview showing which data can be entered, changed and deleted with which applications

☐ Maintaining forms from which data is taken over in automated processing

## 6. Availability Control / Restoration / Reliability / Data Integrity

Ensuring that systems used can be restored in case of a disruption (restorability).

Ensuring that all system functions are available and that any malfunctions are reported (reliability).

Ensuring that saved Personal Information cannot be damaged through system malfunctions (data integrity).

Ensuring that Personal Information is protected from accidental destruction or loss (availability control).

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum:

- □ Uninterruptible Power Supply (UPS)
- □ Devices for monitoring temperature and moisture in server rooms
- □ Fire and smoke detector systems
- □ Alarms for unauthorised access to server rooms
- □ Tests of data restorability
- □ Storing data back-ups in a separate and secure location
- □ In flood areas the server is located above the possible flood level
- □ Air conditioning units in server rooms
- □ Protected outlet strips in server rooms
- □ Fire extinguishers in server rooms
- □ Creating a back-up and recovery concept
- □ Creating an emergency plan

## 7. Separation Control / Separability

Ensuring that data processed for different purposes can be processed separately.

The following technical and organisational measures have been implemented by the Operator for the processing of Personal Information described in this Agreement / Addendum:

- □ Physically separated storing on separate systems or data storage media
- □ Including purpose attributions/data fields in data sets
- □ Establishing database rights
- □ Logical client separation
- □ For pseudonymised data: separation of mapping file and storage on a separate and secured IT system
- □ Separation of production and testing systems