VERGE TECHNOLOGIES (PTY) LTD

(Registration no 2014/163845/07)

3 Mentha Place, Boardwalk Manor Estate,

Pretoria, 0081

South Africa

012 012 5030

hello@verge.co.za

www.verge.co.za

POPIA COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT OF 2013

INDEX

A. INTRODUCTION

The Protection of Personal Information Act (POPI) is intended to balance 2 competing interests. These are:

1. Our individual constitutional rights to privacy (which requires our personal information to be protected); and

2. The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for our company's compliance with POPI.

Where reference is made to the "processing" of personal information, this will include any activity in which the information is worked with, from the time that the information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

B. OUR UNDERTAKING TO OUR CLIENTS:

1. We undertake to follow POPI at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our clients.

2. We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our clients, for this purpose all our clients are required to sign a POPI consent at the start of a transaction, which consent is attached as **Form 1** hereto.

3. Whenever **necessary**, we shall obtain consent to process personal information. (Form 1)

4. Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.

5. We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.

6. We shall collect personal information directly from the client whose information we require, unless:

6.1 The information is of public record, or

6.2 The client has consented to the collection of their personal information from another source, or

6.3 The collection of the information from another source does not prejudice the client, or

6.4 The information to be collected is necessary for the maintenance of law and order or national security, or

6.5 The information is being collected to comply with a legal obligation, including an obligation to SARS, or

6.6 The information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or

6.7 The information is required to maintain our legitimate interests; or

6.8 Where requesting consent would prejudice the purpose of the collection of the information; or

6.9 Where requesting consent is not reasonably practical in the circumstances.

7. We shall advise our clients of the purpose of the collection of the personal information. The purpose of collection of personal information at Verge are to give effect to the scope of work of Verge as follows:

Scope of the Services:

Verge owns and operates the systems DebitSwitch and SwitchTransact which will be provided to the User as in its full functional form as a customised System according to the Users' functional needs.

The Systems shall provide the following core deliverables and components, through a structural methodology further defined and described in Annexure A of the service agreement, annexed hereto as **Form 6.;**

Data Management and storage facility:

A structured database for the indexing, organising and storage and utilisation of Customer data for the application of achieving the organisation's goals and core imperatives;

Structured recording of each Customer's mandate to instruct participation, contact incidents and member/supporter history against a unique identifier which may be used to further structure;

Systems compliance with required and applicable law;

Structured provision of all stored data according to a set schedule as agreed between the parties from time to time for storage by the User;

Payment Collection Facility:

Debit Order Collections;

Card Payment Integrations;

Member Subscription Management;

Billing and Invoice Management;

Enterprise Reconciliation;

Electronic Mandate Management; and

Real-time Analytics and Reporting.

Client Relationship Management ("CRM") Facility:

Automated and manual communication facility via Email and SMS;

Reports and export functionality for Leads and Accounts;

Segmentation of Leads and Accounts;

Import of Leads and Accounts;

Leads and Accounts management;

Integration with Call Centre via an API;

Workflow to manage new and updated Accounts;

Billing and statement management;

Dashboards, automated reporting and manually generated reports;

User administration roles & training (further defined in Annexe A) for assigned staff;

Problem and fault reporting facility – Verge helpdesk;

Methodology and supporter management:

The process and order whereby the Parties agree to the provision of the Services are outlined in a schedule in Annexe A. This process outlines the obligations of the Service Provider.

Systems auditing reports;

SwitchTransact, amongst others:

Provides for effective and efficient revenue collection methods;

Allows for a single deduction in respect of multiple Customer membership

or selected product subscriptions;

Allows for pre-defined action dates automatically combining the debit order reconciliation with the bulk invoice creation on dates agreed by the parties;

Provides effective revenue management through a bank account control mechanism that will provide The User with an efficient basis to monitor cash inflows; distributions and the related financial reporting;

Allows for a Customer identification process by recognising elements such as Customer categorisation, product/campaign or contribution set-up procedures, Payment Method Identification whereby all Customers are given unique debtors accounts, which accounts are capable of storing multiple ledgers for each of the contributions, campaigns, products or subscriptions the Customer has accepted from the User;

Facilitates the seamless inter-functioning between the authorised payment collections and banking switch, incorporating a multi-tiered payment method for revenue collection; utilising sophisticated and growing platform for managing and facilitating a relationship with automated and manual interactions and intelligence gathering through the sophisticated platform offered in SwitchTransact;

Collection of personal information from employees for the purpose of:

a) Making appointments of staff at the firm;

b) Carry out and manage business operations;

c) For staffing, assessment, recruitment and career development Purposes

d) To provide benefits and services to employees

e) For purposes of performance management, succession planning, remuneration and benefits, occupational health administration, corporate security, organizational charts, legal reporting obligations and other legitimate business purposes.

8. We shall retain records of the personal information we have collected for the minimum period as required by law, which is currently **7 years**, unless the client has furnished their consent or instructed us to retain the records for a longer period.

9. We shall destroy or delete records of the personal information (so as to de-identify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired, and a **destruction certificate** shall be obtained from the service provider tasked with the destruction of the personal information.

10. We shall restrict the processing of personal information:

10.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;

10.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;

10.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or

10.4 where the client requests that the personal information be transmitted to another automated data processing system.

11. The further processing of personal information shall only be undertaken:

11.1 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;

11.2 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

11.3 where this is required by the Information Regulator appointed in terms of POPI.

12. We undertake to ensure that the personal information which we collect, and process is complete, accurate, not misleading and up to date.

13. We undertake to retain the physical file and the electronic data related to the processing of the personal information.

14. We undertake to take special care with our client's bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.

15. **Form 1** being the mandate and consent and declaration, referred to in Section O below, and attached hereto, shall be sent to every client when we accept a mandate of any sort, to advise them of our duty to them in terms of POPI.

C. OUR CLIENT'S RIGHTS

1. In cases where the client's consent is required to process their personal information, this consent may be withdrawn. In such instances it must be noted that if consent is withdrawn, we will not be able to fulfill our mandate for which we were appointed. **If the information is needed in terms of legislation, the transaction will not be able to proceed if consent to process the information is not given.**

2. In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing. (Annexure "A")

3. All clients are entitled to lodge a complaint regarding our application of POPI with the Information Regulator at IR@justice.gov.za.

4. **Form 1** referred to in Section O below, and attached hereto, shall be completed by each client when we accept a mandate of any sort, to obtain the client's consent to process their personal information while we render services to them, unless this consent has been obtained within another document signed by the client.

D. SECURITY SAFEGUARDS

1. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, the following security safeguards are implemented:

1.1 Our business premises, where records are kept, are protected by access control, burglar alarms and armed response.

1.2 Archived files are stored behind locked doors and access control to these storage facilities are implemented so that only authorized employees have access to the archived files.

1.3 All the user terminals on our internal computer network and our servers are protected by passwords which are changed on a regular basis.

1.4 Our email infrastructure complies with industry standard security safeguards and meet the General Data Protection Regulation (GDPR), which is standard in the European Union.

1.5 Vulnerability assessments are carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

1.6 All client files and data are protected by encryption of the highest possible levels of electronic security.

1.7 Our staff are trained to carry out their duties in compliance with POPI on a 6-monthly basis.

1.8 It is a term of the contract with every staff member that they must maintain full confidentiality in respect of all our clients' affairs, including our clients' personal information. Personal information

includes an obligation on the staff member (1) to maintain the firm's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to acquired by any unauthorised person. See **Form 5** attached hereto that is an addendum to all our employment contracts.

1.9 The processing of the personal information of our staff members must take place in accordance with the rules contained in the relevant labour legislation.

1.10 The use of information systems by employees are regulated by our **Internal manual & Fair Usage Policy**, attached hereto. **(Form 5)**

1.11 The digital work profiles and privileges of staff who have left out employ are properly terminated.

1.12 The personal information of clients and staff are destroyed timeously in a manner that de-identifies the person.

1.13 We have a Disaster Recovery Plan, which includes a business continuity and sustainability plan for any unforeseen disastrous events, which plan is attached hereto as **Form 4**.

When the Disaster Recovery Plan is implemented, all employees must still adhere to all stipulations as set out in this manual.

2. These security safeguards are verified on a regular basis to ensure effective implementation, and these safeguards continually updated in response to new risks or deficiencies.

E. SECURITY BREACHES

1. Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, the Information Regulator and the relevant client/s will be notified, unless we are no longer able to identify the client/s. This notification must take place as soon as reasonably possible.

2. Such notification is firstly given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed.

3. The notification to the client must be communicated in writing within 48 hours (2 business days) in one of the following ways, with a view to ensuring that the notification reaches the client:

3.1 By mail to the client's last known physical or postal address;

3.2 By email to the client's last known email address;

3.3 By publication on our website or in the news media; or

3.4 As directed by the Information Regulator.

4 This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:

4.1 A description of the possible consequences of the breach;

4.2 Details of the measures that we intend to take or have taken to address the breach;

4.3 The recommendation of what the client could do to mitigate the adverse effects of the breach; and

4.4 If known, the identity of the person who may have accessed, or acquired the personal information.

F. CLIENTS REQUESTING RECORDS

1. On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

2. If we hold such personal information, on request, and upon payment of a fee of **R700.00 plus VAT**, we shall provide the person with the record, or a description of the personal information, including information about the

identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period of time, in a reasonable manner and in an understandable form.

3. A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form. See **Form 4** attached hereto.

4. In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.

5. In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or his delegate) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6. If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

G. THE CORRECTION OF PERSONAL INFORMATION

1. A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

2. A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.

3. Any such request must be made on the prescribed form, (Annexure "B"), referred to in Section O below.

4. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

5. In the event that a dispute arises regarding the client's rights to have information corrected, and in the event that the client so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

6. We must notify the client who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

H. SPECIAL PERSONAL INFORMATION

1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

2. We shall not process any of this special personal information without the client's consent, or where this is necessary for the establishment, exercise or defense of a right or an obligation in law.

3. Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information, but should it be necessary the guidance of the Information Officer, or their deputy/delegate, must be sought.

I. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

1. We may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

J. INFORMATION OFFICER

1. Our Information Officer is Eddy Marais who is the sole proprietor of the firm. Our Information Officer's responsibilities include:

1.1 Ensuring compliance with POPI.

1.2 Dealing with requests which we receive in terms of POPI.

1.3 Working with the Information Regulator in relation to investigations.

2. Our Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above. Such designation shall be done by the completion of the prescribed form a copy of which is an annexure to this Compliance Manual, see **Form 2** attached hereto.

3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties.

4. In carrying out their duties, our Information Officer must ensure that:

4.1 This Compliance Manual is implemented;

4.2 A Personal Information Impact Assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

4.3 That this compliance manual is developed, monitored, maintained and made available;

4.4 That internal measures are developed together with adequate systems to process requests for information or access to information;

4.5 That internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and

4.6 That copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

5. Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer must familiarize themselves with the content of these notes.

K. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

1. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:

1.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

1.3 if we are processing information for the purposes of credit reporting (this will be important if we are making reports to assist with tenant profiling, for example, to TPN or Transunion ITC, Experian and/or any other credit bureau).

1.4 if we are transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

2. The Information Regulator must be notified of our intention to process any personal information as set out in paragraph 1.1 above prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator,

which must not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

L. DIRECT MARKETING

1. We may only carry out direct marketing (using any form of electronic communication) to clients if:

1.1 they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

1.2 they did not object then or at any time after receiving any such direct marketing communications from us.

1.3 We confirm that we from time to time sent out articles that is sent out via e-mail to all our clients in our CRM, containing our marketing tools/materials, and included in such email is an option to opt-out of the weekly e-mails.

2. We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our conveyancing and other legal services, and we may then only market our legal services to them.

3. We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

4. We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

5. All direct marketing communications must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

M. TRANSBORDER INFORMATION FLOWS

1. We may not transfer a client's personal information to a third party in a foreign country, unless:

1.1 The client consents to this, or requests it; or

1.2 Such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or

1.3 The transfer of the personal information is required for the performance of the contract between ourselves and the client; or

1.4 The transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between ourselves and the third party; or

1.5 The transfer of the personal information is for the benefit of the client, and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

N. DATA PRIVACY CONTROLS

1. Privacy Policy

1.1 This Privacy Policy describes our firm's policies and procedures on the collection, use and disclosure of your information when you use the service and tells you about your privacy rights and how the law protects you.

1.2 We use your personal data to provide and improve our service to you. By using the firm's service, you agree to the collection and use of information in accordance with this privacy policy.

2. Interpretation and Definitions

2.1 Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

2.2 Definitions

For the purposes of this Privacy Policy:

- **Account** means a unique account created for you to access our services or parts of our services.
- **Firm** (referred to as either "the firm", "We", "Us" or "Our" in this Agreement) refers to Verge.
- **Country** refers to: South Africa.
- **Device** means any device that can access the services such as a computer, a cellphone or a digital tablet.
- **Personal Data** is any information that relates to an identified or identifiable individual.

- **Services** refers to all the legal services our firm offers, as well as access to our website and the functionalities and downloads thereon.

- **Service Provider** means any natural or legal person who processes the data on behalf of the firm. It refers to third-party companies or individuals employed by the firm to facilitate the services, to provide the services on behalf of the firm, to perform services related to our services or to assist the firm in analyzing how the services are used.

- **Usage Data** refers to data collected automatically, either generated by the use of our services or from the service infrastructure itself (for example, the duration of a page visit).

- **Website** refers to the firm's website, accessible from switchtransact.com and sub-domains.
- **You** mean the individual accessing or using our services, or the company, or other legal entity on behalf of which such individual is accessing or using our services, as applicable.

2.3 Personal Data

While using our services, we may ask you to provide us with certain personal identifiable information that can be used to contact or identify you, as well as information as required in terms of the

Financial Intelligence Centre Act 38 of 2001 (FICA). Personal identifiable information may include, but is not limited to:

- Email address;
- First name and last name;
- Identity number;
- Phone number;
- Physical and Postal Address;
- Usage Data.

2.4 Usage Data

Usage data is collected automatically when using our services.

Usage data may include information such as your device's internet protocol address (e.g. IP address), browser type, browser version, the pages of our website that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access our services/website by or through a mobile device, we may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your

mobile operating system, the type of mobile internet browser you use, unique device identifiers and other diagnostic data.

We may also collect information that your browser sends whenever you visit our website or communicate electronically or when you access the service by or through a mobile device.

3. Use of Your Personal Data

The firm may use personal data for the following purposes:

- **To provide and maintain our services**, including to monitor the usage of our services.
- **To manage your account or active transactions with the firm:** The personal data you provide can will enable the firm to provide you with the services we were mandated for, and to enable us to comply with the necessary compliance legislation in place such as FICA and POPIA.
- **For the performance of a contract:** the development, compliance and enforcement of necessary transactions we are attending to for example. the sale agreement, the mortgage loan agreement etc.
- **To contact you:** To contact you by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or

informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.

- **To provide you** with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information.

- **To manage your requests:** To attend and manage your requests to us.

- **For other purposes**: We may use your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our service, products, services, marketing and your experience.

We may share Your personal information in the following situations:

- **With Service Providers:** We may share your personal information with service providers in order for us to give effect to our mandate to attend to your transaction, including but not limited to our software vendors, SARS, the city council, the courts of South Africa.

- **With Affiliates:** We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy

policy. Affiliates include our parent company and any other subsidiaries, joint venture partners or other companies that we control or that are under common control with us.

- **With business partners:** We may share your information with our business partners to offer you certain products, services or promotions.

- **With other users:** when you share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside.

- **With Your consent**: We may disclose your personal information for any other purpose with your consent.

4. Retention of Your Personal Data

The Company will retain your personal data only for as long as is necessary for the purposes set out in this privacy policy or as set out by legislation, currently in terms of the prevailing legislation your information must retained for a period of **7 years**.

5. Transfer of Your Personal Data

Your information, including personal data, is processed at the firm's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be

transferred to — and maintained on — computers located outside of your province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

Your consent to this privacy policy followed by your submission of such information represents your agreement to that transfer.

The firm will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy and no transfer of your personal data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

6. Disclosure of Your Personal Data

6.1 Law enforcement

Under certain circumstances, the firm may be required to disclose your personal data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

6.2 Other legal requirements

The firm may disclose your personal data in the good faith belief that such action is necessary to:

- Comply with a legal obligation;

- Protect and defend the rights or property of the firm;
- Prevent or investigate possible wrongdoing in connection with the services rendered;
- Protect the personal safety of users of the service or the public;
- Protect against legal liability;

7. Security of Your Personal Data

The security of Your Personal Data is important to us but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, we cannot guarantee its absolute security.

7.1 Children's Privacy

In the event that any client is a minor we will only collect personally identifiable information from such client with the consent of his/her parents or guardians, as their consent is always needed in the conclusion of a transaction with a minor within our legal scope. If you are a parent or guardian and you are aware that your child has provided us with personal data without your consent, please contact us.

7.2 Links to Other Websites

Our services and or website may contain links to other websites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the privacy policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

7.3 Changes to this Privacy Policy

We may update our privacy policy from time to time. We will notify you of any changes by posting the new privacy policy on this page.

7.4 Contact Us

If you have any questions about this privacy policy, you can contact us:

- By email: legal@verge.co.za
- By phone number: 012 012 5030

O. SCHEDULE OF ANNEXURES AND FORMS

1. Client's consent to process personal information, mandate and declaration as an Addendum to **Verge Services Agreement**. (Form 1)

2. Designation and delegation to Deputy Information Officer. (Form 2)

3. Authorization of Information Officer. (Form 3)

4. Disaster Management Plan (Form 4)

5. Internal Manual & Fair Usage Policy (Form 5)

6. Service Agreement (Form 6)

A. Objection to the Processing of Personal Information (Form 1 of the Regulations). (Annexure "A")

B. Request for correction or deletion of personal information (Form 2 of the Regulations). (Annexure "B")

Verge Technologies (Pty) Ltd

July 2021