commsure
FINANCIAL SOLUTIONS

Protection of Personal Information Policy

Table of Contents

1. Definitions

For purposes of this policy, the below mentioned words and/or phrases shall have the following meaning assigned to them:

2.1. **"child''** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself;
2.2. **"competent person''** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
2.3. **''consent''** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
2.4. **"Constitution"** means the Constitution of the Republic of South Africa, 1996;
2.5. **''data subject''** means the person to whom personal information relates e.g. policyholders, employees, intermediaries, consultants, juristic person etc;
2.6. **"intermediaries"** means any person rendering services as an intermediary;
2.7. **"personal information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
2.7.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
2.7.2. information relating to the education or the medical, financial, criminal or employment history of the person;
2.7.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
2.7.4. the biometric information of the person;
2.7.5. the personal opinions, views or preferences of the person;
2.7.6. 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;
2.7.7. the views or opinions of another individual about the person; and
2.7.8. 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;
2.8. **"POPI"** stands for Protection of Personal Information Act, 2013 (Act No. 4 of 2013);
2.9. **"processing''** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-
2.9.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
2.9.2. dissemination by means of transmission, distribution or making available in any other form; or
2.9.3. merging, linking, as well as restriction, degradation, erasure or destruction of information.
2.10. **"Regulator''** means the Information Regulator as established by section 39 of POPI.
2.11. "third parties" intermediaries, binder holders, companies in our group of companies, contractors and verification agencies.

2. Policy Statement

2.1. This policy gives effect to our commitment to process information in accordance with the mandate obtained from the data subject and any obligatory nature, subject to complying with

the Protection of Personal Information Act of 2013, "POPIA". This policy is not limited to complying with provisions of POPIA, this extends to information governance in general and standards that the Board deems relevant for effective information governance.

2.2. We further commit to comply with POPIA, not just in letter, but in spirit as well. We understand the intent behind the introduction of the legislation and therefore we are embracing this as it is seeking to ensure privacy and structured way of information management.

3. Introduction

3.1. As an authorised financial service provider, Commsure has a legal duty to ensure that all personal information it processes, is lawfully processed in terms of the conditions for lawful processing of personal information as highlighted in POPIA.

3.2. Furthermore, this document sets out specific duties for Commsure in processing data subject personal information, from when it is collected or sourced until the information is of no more use and needs to be destroyed.

4. Processing personal information

4.1. Commsure is required to process personal information to enter into contracts, to fulfil contractual requirements and to fulfil its regulatory obligation. The company further processes personal information to enable it to enhance the experience of the data subject in relation to the business relationship. To ensure that data subject is always treated fairly and in promoting transparency, Commsure will disclose up-front the purpose of processing the personal information obtained and what it may further be used for.

4.2. Where information may potentially be used for other objectives than originally acquired for, Commsure will, prior to processing the personal information, obtain a consent from the data subject concerned. Commsure may however process personal information in absence of a consent if processing is required to:

4.2.1. exercise a contractual or legal obligation;

4.2.2. processing is required to protect the legitimate interest of the data subject;

4.2.3. processing is necessary for pursuing the legitimate interest of Commsure or third-party contracted to Commsure.

4.3. Personal information will only be collected from a consenting adult, competent person or from a third party, subject to valid consent from the data subject.

5. How we will collect personal information

5.1. Commsure will primarily collect personal information directly from the data subject, which would typically be face-to-face, via other channels like emails, telephone and website.

5.2. Personal information may also be collected from third parties, however, the data subject consent will be requested prior to executing on this action. Commsure will clearly advise the data subject why this action may be necessary.

5.3. Commsure will never request personal information on the social media accounts except where 6.1 above applies.

6. How your personal information will be processed?

6.1. The following are some of the reasons for processing personal information:

6.1.1. Compliance with law, in letter and spirit;

6.1.2. To fulfil a contractual obligation;

6.1.3. To enhance the data subject's experience;

6.1.4. For general marketing;

6.1.5. For research and product development or enhancement; and

6.1.6. Protecting the data subject's legitimate interests.

7. Cross border information

7.1. Commsure will never transfer personal information deemed confidential, unless this is public knowledge, to any entity outside the Republic of South Africa. Where an obligation arises to transfer personal information outside the republic, the data subject will be accordingly notified.

8. Disclosure of personal information

8.1. Commsure may share any personal information of a data subject with a third party contracted to perform services approved by Commsure in terms of contractual agreement. In such instances, Commsure will ensure that third parties have the relevant controls in place to comply with the conditions for lawful processing of personal information.

8.2. Commsure may also disclose any personal information when it has a duty or right to do so in terms of legislation or in any legal proceedings.

9. Retention and deleting of personal information

9.1. Commsure will not retain records of personal information any longer than is necessary for achieving the purpose for which the information was collected or processed, unless:

9.1.1. the retention of such record is required by law;

9.1.2. Commsure requires such record for lawful purposes related to its function or activities;

9.1.3. the retention of such record is required in terms of a contractual agreement between the parties thereto; or

9.1.4. the necessary consent has been obtained from the data subject and is for a legitimate interest

9.2. Commsure will destroy or delete a record of personal information as soon as reasonably practicable, where it is no longer authorised to retain such record.

10. Security safeguards

10.1. Commsure will ensure that all the information that gets processed is adequately safeguarded to ensure that the integrity of information is maintained and that there is proper access control.

10.2. Where Commsure makes use of third parties to process personal information, Commsure will ensure that that the third parties have adequate control measures in place.

10.3. Should there be reasonable grounds to believe that the personal information has been accessed or acquired by any unauthorised person, Commsure will take immediate steps to mitigate any risk that might be suffered by the data subject and will notify the Regulator and impacted data subject of such breach including mitigations in writing.

11. The rights of a data subject

The data subject has the right to lawful processing of their personal information in terms of the provisions of POPI, including the right to:

11.1. Be made aware when personal information is collected, accessed or acquired by an unauthorised person;

11.2. Inquire whether Commsure holds personal information of the data subject and to request access to the personal information;

11.3. Withdraw consent; provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information required to exercise legitimate obligation as provided by POPI will not be affected.

11.4. Request, where necessary, the correction, destruction or deletion of personal information (*through sending Form 2*);

11.5. Object on reasonable grounds relating to a particular situation to the processing of your personal information (*through sending Form 1*);

11.6. Object to the processing of personal information at any time for purposes of direct marketing or unsolicited electronic communications (*through sending Form 1*);

11.7. Not to have personal information processed for purposes of direct marketing by means of unsolicited electronic communications;

11.8. Not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of personal information intended to provide a profile that may subject the data subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct;

11.9. The provisions of subsection 12.8 do not apply if the decision—

11.9.1. has been taken in connection with the conclusion or execution of a contract, and—

11.9.1.1. the request of the data subject in terms of the contract has been met; or

11.9.1.2. appropriate measures have been taken to protect the data subject's legitimate interests;

or

11.9.2. is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

11.10. The appropriate measures, referred to in subsection 12.9, must—

11.10.1. provide an opportunity for a data subject to make representations about a decision referred to in subsection 12.8; and

11.10.2. require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of 12.10.1.

11.11. Submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject (*through sending Form 5*);

11.12. Institute a civil action for damages against Commsure, in a court with competent jurisdiction, for breach of any of the provisions of POPI.

12. Limitation

12.1. Commsure processes personal information of children to the extent allowed to fulfil its contractual obligation and where there is a legal obligation to disclose that information. Commsure does not directly engage or enter into contract with minors.

12.2 Commsure will not be processing the following special personal information, unless it is required to do so by law and where it is essential to enter into contract as part of risk mitigation to the business. The following is examples of special personal information:

12.2.1. the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject;

12.2.2. the criminal behaviour of a data subject to the extent that such information relates to— the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

13. Reporting

13.1 For any questions or where further information may be required, details provided on Annexure A.

13.2 Any violations or complaints may be reported to the Information Regulator, details provided on Annexure A

14. Review of this policy

Amendments to or review of this policy will take place on an ad hoc basis or at least once a year.

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	

C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/designated person

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	

Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/ designated person

FORM 5

COMPLAINT REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION/COMPLAINT REGARDING DETERMINATION OF AN ADJUDICATOR IN TERMS OF SECTION 74 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 7]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Complaint regarding:

☐ Alleged interference with the protection of personal information

☐ Determination of an adjudicator.

PART I	**ALLEGED INTERFERENCE WITH THE PROTECTION OF THE PERSONAL INFORMATION IN TERMS OF SECTION 74(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (Act No. 4 of 2013)**
A	**PARTICULARS OF COMPLAINANT**
Name(s) and surname / registered name of data subject:	
Unique Identifier/Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address :	

B	**PARTICULARS OF RESPONSIBLE PARTY INTERFERING WITH PERSONAL INFORMATION**
Name(s) and surname/ Registered name of responsible party:	

Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR COMPLAINT***(Please provide detailed reasons for the complaint)*
PART II	**COMPLAINT REGARDING DETERMINATION OF ADJUDICATOR IN TERMS OF SECTION 74(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)**
A	**PARTICULARS OF COMPLAINANT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	

B	PARTICULARS OF ADJUDICATOR AND RESPONSIBLE PARTY
Name(s) and surname of adjudicator:	
Name(s) and surname of responsible party /registered name:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR COMPLAINT** *(Please provide detailed reasons for the grievance)*

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/ designated person

Annexure A - Incident Response Plan

1. **Introduction**
   This incident response plan is to guide employees how to respond to an incident or suspected incident which is in the form of a breach in personal information held or hosted by Commsure, directly or indirectly. This further demonstrates to the data subject, how breaches in personal information will be treated and the issuance of any notifications where may be required.
2. **Incident**
   An incident/breach is an event where data, especially personal information, gets accessed by an unauthorised user or where this is suspected to have been accessed by an unauthorised user. Any other security compromise to data is also considered as an incident or data breach.
3. **Lodging an incident**
   All incident identified or suspected must be reported to the Information Officer immediately upon discovery or suspicion. The Information Officer must then instantaneously report this to Risk Committee. (Information Officer and Risk Committee to determine reporting format.
4. **Management of lodged incidents.**
   - 4.1. All lodged incidents will be investigated to validate the allegation/suspicion. Depending on the magnitude and nature of investigation required, third parties may be onboarded as part of the investigation team.
   - 4.2. As part of the investigation, Commsure may be required to further process personal information of data subjects. Irrespective of this, Commsure ensure to the protection of personal information, even where it is processed further.
   - 4.3. On conclusion of the investigation, Commsure will communicate with the relevant parties depending on the nature of the outcome.
5. **Communication of outcome**
   - 5.1. Where a threat has been identified depending on the magnitude of the threat, Commsure will timeously inform the following parties:
     - 5.1.1. The Information Regulator on:
       - 5.1.1.1. Breach, detailed description of this breach
       - 5.1.1.2. Extent of the breach
       - 5.1.1.3. Actions already taken to mitigate and remediate the situation
       - 5.1.1.4. Actions still to be taken, and
       - 5.1.1.5. The respective timelines of the above actions
     - 5.1.2. Data subject on:
       - 5.1.2.1. Breach, detailed description of this breach
       - 5.1.2.2. Extent of personal information of the data subject that was breached
       - 5.1.2.3. Recommended actions or non-actions to be taken by the data subject to mitigate the possible adverse effects of the security compromise,
       - 5.1.2.4. Respective timelines where applicable. and
       - 5.1.2.5. if known, the identity of the unauthorised person who may have accessed or acquired the personal information.
     - 5.1.3. Other parties with interest to the breach will also be notified where applicable. Some examples would be SAPS, insurer, etc. This will be dependent on the nature of the breach.

5.2. It is critical that the relevant parties be informed as soon as possible so that they can take the necessary precautions where require. Investigations in nature takes a while to conclude, as result the delay could aggravate the situation. Commsure will as soon as reasonably possible, even before the conclusion of any investigation, where it can confidently confirm the breach, immediately communicate/inform the relevant parties of the breach. This communication will be sent out within 48 hours of positively identifying the breach.

6. Closure

6.1. Commsure will further investigate, where required, to establish the root cause of the breach or the causal event and notify the relevant authorities where applicable.

6.2. Further case studies will be conducted to find a suitable mitigation as well as remediation of the risk that occurred.

6.3. Commsure will communicate with affected parties to provide the outcome if not already provided.

Annexure B – Contact details

Information Officer
Gail Schouw
Commsure Financial Solutions (Pty) Ltd
14 College Road
Rondebosch
7700
Tel: 021 685 0070
Enquiries: gail.schouw@commsure.co.za
Complaints: gail.schouw@commsure.co.za

The Information Regulator (South Africa)
33 Hoofd Street
Forum III, 3rd Floor Braampark
Braamfontein, Johannesburg
Tel: 010 023 5207
Fax: Not available as yet
Complaints: complaints.IR@justice.gov.za
General enquiries: inforeg@justice.gov.za