28 September 2015

Norton Rose Fulbright South Africa Inc
15 Alice Lane
Sandton 2196
South Africa

Tel +27 11 685 8500
Fax +27 11 301 3200

Direct fax +27 11 301 3200
PO Box 784903 Sandton 2146
Docex 215 Johannesburg
nortonrosefulbright.com

Direct line
+27 11 685 8929

Email
kerri.crawford@nortonrosefulbright.com

Your reference J Schubart
Our reference INS140

By Email: jwsch@telkomsa.net

Mr Jan Schubart

Institute of Loss Adjusters of Southern Africa

Dear Jan

Opinion: compliance with the Protection of Personal Information Act (POPI)

1 Introduction

1.1 We were asked to draft a generic consent in terms of the *Protection of Personal Information Act, 2013* (**POPI**) for use by loss adjusters when engaging with insureds.

1.2 Loss adjusters do not need consent to investigate a claim or to collect and use the insured's personal information in the course of those investigations. Our detailed views are below. In summary:

(1) The collection and use of insureds' personal information in investigating claims is permitted without consent, as it is necessary to perform the insurance contract or is in the insurer's legitimate interests.

(2) Loss adjusters acting in terms of a mandate from the insurers have limited compliance obligations. However, POPI requires the insurers to contractually impose certain obligations on mandated loss adjusters and they are likely to request amendments to agreements to this effect.

(3) Loss adjusters acting without a formal mandate or beyond its scope must comply with all of the requirements for lawful processing under POPI, including information security, retention, notification and sensitive information and cross-border transfer requirements.

(4) If loss adjusters process insured's personal information for purposes other than their mandate to investigate claims, consent may be required if the processing cannot be justified on other grounds.

1.3 The operative provisions of POPI are not yet in force. However if loss adjusters are reviewing their information handling practices now, it would be prudent to align them with POPI rather than having to repeat the exercise once these provisions become law. If insurers are implementing their compliance programmes, they will in all likelihood require loss adjusters to demonstrate their compliance.

1.4 We have produced a short brochure which can be given to loss adjusters to inform them of their obligations. If you are happy with the content, we suggest discussing a joint branding initiative.

2 Does POPI apply to loss adjusters?

2.1 POPI applies to all entities which process personal information in South Africa. **Processing** is anything that is done with the personal information, including collection, storage, use, sharing and deletion.

2.2 **Personal information** has a wide meaning and includes any information that identifies and relates to living individuals and existing corporates. The **data subject** is the individual or corporate to whom the personal information relates, namely the insured.

2.3 The information collected and used by loss adjusters in investigating claims inevitably includes personal information (such as contact details, ID numbers and company registration numbers, unique identifiers such as policy numbers and financial information). Compliance with POPI is therefore required.

3 Responsible parties or operators?

3.1 POPI places different obligations on principals and their agents or service providers.

(1) The **responsible party** is the entity which determines the purpose of and means for processing personal information. This entity must comply with all of the requirements for lawful processing in POPI.

(2) An **operator** processes personal information for a responsible party in term of a contract or mandate, without coming under the direct authority of the responsible party. Operators have limited obligations under POPI (see paragraph 4).

3.2 If loss adjusters act in terms of a mandate from the insurers to investigate claims, they are operators in relation to the personal information used for this purpose. The insurers are the responsible parties.

3.3 In practice, loss adjusters often receive telephonic instructions to investigate claims. This is no less a mandate than a formal written instruction, but it may lead to difficulties in establishing the scope of the mandate. This is relevant because loss adjusters who act outside the scope of their mandate are responsible parties, not operators. This gives them greater compliance obligations. We deal with this in more detail below.

3.4 It is possible for a loss adjuster to be an operator and a responsible party.

4 Loss adjusters acting under mandate (operators)

4.1 As mentioned, operators have limited obligations under POPI.

(1) Loss adjusters acting under a mandate may process personal information of insureds only with the knowledge or authorisation of the insurer and may not disclose this information to any third party unless required by law or in the proper performance of their duties.

(2) They must notify the insurer immediately if there are reasonable grounds to believe that insureds' personal information has been accessed or acquired by an unauthorised person. The insurers must be notified even if the data breach has not yet been confirmed. The insurer has reporting obligations to the Regulator and insureds, which depend on loss adjusters reporting to them.

4.2 Provided that loss adjusters do not process personal information of insureds outside of the scope of their mandate or otherwise without the insurer's authorisation and comply with the notification obligations, they are compliant with POPI in respect of this information.

4.3 POPI contains various grounds on which responsible parties may process personal information, including performance in terms of a contract, legitimate interests and consent. The responsible party must ensure that one of these grounds exists before instructing the operator. Operators do not need any ground of their own to process personal information in terms of their mandate. Insurers would typically rely on the grounds that the processing of personal information is necessary to perform the

contract of insurance or to protect the insurer's legitimate interests. The insurer does not need to obtain consent.

4.4 POPI does however require insurers to impose certain obligations on loss adjusters regarding the security of the personal information in terms of a written contract (see paragraph 6). Loss adjusters are likely to receive requests to amend their contracts as the insurers address their POPI compliance. Loss adjusters without written contracts are likely to be required by insurers to conclude them.

4.5 Because the insurers are liable under POPI for processing activities which loss adjusters perform on their behalf, they may also request clauses in their contracts with loss adjusters:

(1) requiring compliance with the operator requirements mentioned in paragraph 4.1;

(2) requiring cooperation and assistance with any assessments or investigations conducted by the Regulator and compliance with any directions of the Regulator, including making public announcements regarding data breaches;

(3) indemnifying the insurers against any damages (including administrative fines imposed by the Regulator) arising from breach of the loss adjusters obligations.

4.6 In negotiating data privacy clauses with insurers, loss adjusters should request an exclusion of liability for indirect damages and negotiate a reasonable cap on direct damages. Note that the maximum administrative fine which the Regulator may impose is R10 million.

4.7 We also recommend recording in the agreement that the insurer must comply with POPI in relation to personal information for which they are the responsible party. Ideally we would recommend an indemnity in favour of the loss adjuster for damages suffered as a result of the insurer's breach of POPI, but we expect that most insurers will reject this.

5 Loss adjusters acting without mandates

5.1 Acting outside of a mandate makes the loss adjuster a responsible party in relation to those actions which are outside of the mandate. In this event, loss adjusters would need to comply with the obligations of responsible parties, including having their own ground of justification to process the personal information.

5.2 Loss adjusters acting as responsible parties would need to assess whether their processing is justified on grounds such as their own or the insureds' legitimate interests or where the processing complies with a law. If not, the loss adjuster would need to obtain the insureds' consent directly.

5.3 Regardless of the purpose, loss adjusters acting without or beyond their mandates must comply with all of the requirements for lawful processing with which a responsible party must comply, including:

(1) information security and retention of records (*dealt with in paragraphs 6 and 7*);

(2) notification obligations – responsible parties must take reasonably practical steps to make data subjects aware of various matters when collecting their personal information; and

(3) cross-border transfer requirements - there are limited circumstances in which personal information may be transferred out of South Africa.

6 Information security

6.1 Loss adjusters acting under mandate are likely to receive requests from insurers to conclude or amend agreements, because the insurers are required to contractually oblige the loss adjusters to take the same measures to secure personal information as they are required to take under POPI. Loss adjusters acting without mandate are statutorily required to take these measures as responsible parties.

6.2 Responsible parties must take technical and organisational measures to protect personal information against loss, damage, unauthorised destruction and unlawful access. POPI does not prescribe specific measures, but states that they must be appropriate and reasonable. The measures taken will be regarded as appropriate and reasonable if they:

(1) identify all reasonably foreseeable internal and external risks to personal information;

(2) establish and maintain appropriate safeguards against the risks identified;

(3) include regular verification that the safeguards are effectively implemented;

(4) include continual updating of the safeguards in response to new risks or deficiencies in existing safeguards.

6.3 Generally accepted information security practices and procedures, whether generally applicable or industry specific must be taken into account.

6.4 Technical measures include IT security and the security of physical records. Organisational measures include establishing and enforcing information security policies and procedures and ensuring that all staff with access to personal information are trained in how to handle it in compliance with POPI.

7 Retention of records

7.1 POPI does not prescribe specific retention periods. Personal information may not be retained longer than is necessary to fulfil the purpose for which it is processed. There are exceptions, such as where longer retention is authorised by law or a contract with the data subject, or with the data subject's consent.

7.2 Records relating to claims investigations may need to be retained after the report is submitted to the insurer for use in litigation. Once a claim is settled and the file is closed, the record should be destroyed after a reasonable time, having regard to the nature of the claim, prescription and any prescribed retention periods in other laws.

7.3 Retention of records should be dealt with in the contract between insurer and loss adjuster. Loss adjusters acting without or beyond a mandate would need to ensure compliance themselves.

8 Sensitive information

8.1 Additional requirements apply to categories of special personal information (namely information concerning religious beliefs, race, trade union membership, health or sex life, biometrics and criminal offences) and personal information of children. This information may only be processed in limited circumstances authorised by POPI.

8.2 Loss adjusters acting under mandate do not need their own authorisation to process sensitive information. As mentioned, we recommend that the agreement or mandate requires the insurers to comply with their obligations under POPI, which includes having this authorisation.

8.3 Loss adjusters acting without or beyond a mandate would need to ensure that they are authorised under POPI to process any sensitive information.

Yours faithfully

Kerri Crawford
Associate
Norton Rose Fulbright South Africa Inc
Directors: Donald Dinnie / Rohan Isaacs