NON-LIFE INSURANCE DATA REQUIREMENTS

A GUIDELINE FOR THE TRANSFER OF DATA CONTENT[1] PREPARED BY THE SOUTH AFRICAN INSURANCE ASSOCIATION (SAIA), THE FINANCIAL INTERMEDIARIES ASSOCIATION OF SOUTHERN AFRICA (FIA) AND THE SOUTH AFRICAN UNDERWRITING MANAGERS ASSOCIATION (SAUMA)

VERSION
01

[1] The difference between Data and Data content:
Data is a raw fact or value; a "given." It is a unit of information that is self-referencing and circular. (e.g. Carpenter)
Data content is contextualized data. Context situates data within a system of values, concepts, and expressions.
From a data content management perspective, data alone lacks the proper variables or taxonomical structures to produce content fit for processing or automation. Data content helps provide a clearer perspective in analyzing, categorizing, and producing valuable information. (e.g. Policyholder surname: Carpenter)

TABLE OF CONTENTS

PART 1

POLICYHOLDER, POLICY AND CLAIMS

INTRODUCTION

These guidelines are designed to provide direction with regards to the **minimum requirements** for the transfer of data content between non-life insurers and third parties that render outsourced services (including binder services) to those insurers in terms of the relevant regulatory requirements. The use of the term "binder holder" in the context of data transfer throughout this document (apart from use in regulatory extracts) includes all such third parties which render outsourced services to the non-life insurers. These guidelines are intended to achieve more clarity and certainty about what minimum data content within data content areas[2] need to be transferred in order to ensure a more consistent approach to data transfer across the industry.

The guidelines do not intend to replace any more detailed data exchange solution but rather to provide in plain language the foundational and minimum requirements upon which any such solution must be based and be able to demonstrate alignment.

As such the framework is provided at a high level with notes regarding the general description and / or purpose of certain data content to guide the reader as to the intention and is the minimum information required to be transferred to the insurer. Data transfer files need not follow the sequence or format set out in this document but must contain all the data content areas in the document to facilitate regulatory review and inspection for compliance purposes.

The data content and data content areas set out in these guidelines are intended to provide in commercial terms an indication of the minimum regulatory requirements. Precise data specifications for information to be transferred as data content must be agreed between individual insurers and binder holders / outsourced service providers and may also include additional data content over and above these minimum requirements.

[2] Data content area – a logical group of data content (e.g.; Policyholder information is a data content area whilst Policyholder surname is data content).

REGULATORY REQUIREMENTS

The founding regulatory principles for the transfer of Policyholder and Policy data and data content are contained in the following extracts:

REGULATIONS UNDER THE SHORT-TERM INSURANCE ACT, 1998

Definitions

6.1
"…
(i) "integration" means policy and policyholder data is in a format that is readily recognisable and capable of being meaningfully utilised immediately by the core insurance systems and applications of the insurer;"

Governance and oversight requirements
6.2A (1) An insurer must before entering into a binder agreement and at all times thereafter –

(a) have the necessary resources and ability to exercise effective oversight over the binder holder on an ongoing basis, particularly in respect of identifying, assessing, managing and reporting on the risks of poor customer outcomes arising from conducting insurance business through binder agreements;

(b) satisfy itself of the adequacy of the binder holder's –

(i) governance, risk management and internal control framework, including the binder holder's ability to comply with applicable laws and the binder agreement; and

(ii) fitness and propriety, including any specific technical expertise required to perform the function to which the binder agreement relate;

(c) have documented controls in place to ensure the validity, accuracy, completeness and security of any information provided by the binder holder; and

(d) have appropriate contingency plans in place to address any shortcomings it may identify that could lead to it not being satisfied as to the matters provided for in paragraph (b), including where the binder holder is unable to provide the insurer with the relevant data in the appropriate format.

(2) An insurer must before entering into a binder agreement and at all times thereafter be satisfied that the binder holder has the operational ability to ensure integration between the information technology system of the insurer and the information technology system of the binder holder, which enables the insurer to have access[3] to up-to-date, accurate and complete data held by the binder holder as and when requested by the insurer and as required in terms of the binder agreement and any other regulatory requirements relating to data management, including the requirements in the Policyholder Protection Rules;

(3) An insurer must regularly review and, where appropriate, act upon the information received from the binder holder to assess the appropriateness and suitability of the functions being performed in terms of the binder arrangement in delivering fair outcomes to policyholders on an ongoing basis.";

6.3(1)

(d) require that the binder holder at all times is fit and proper, and has appropriate governance, risk management, internal controls and information technology systems in place to render the services under the binder agreement;";

(k) specify that the insurer has a right to access any data held by the binder holder as and when such data is requested by the insurer;
….

(p) require the binder holder to provide the insurer with access to up-to-date, accurate and complete data (in accordance with Regulation 6.2A (2)) on a daily basis to ensure that the insurer is able to comply with any regulatory requirements relating to data management, including any requirements provided for in the Policyholder Protection Rules;"

POLICYHOLDER PROTECTION RULES (PPRs), 2017

Chapter 6, Rule 13: Data Management, under the following subsections, refer to the requirements for data content:

[3] Access (which would include amongst other things actual data transfer and access to the IT platform of the binder holder) will suffice if such access meets the integration requirements contained in Regulation 6.2A(2). This will include providing an insurer with unfettered access to a cloud-based system. (FSCA comment in the Comments Matrix - National Treasury's responses to comments on Short-Term Insurance Act, 1998: Proposed amendment of Regulations made under Section 70)

"13.3 An insurer must have an effective data management framework that includes appropriate strategies, policies, systems, processes and controls relating to the processing of any data which enables the insurer at all times to –

(a) have access, as and when required, to data that is up-to-date, accurate, reliable, secure and complete;

(b) properly identify, assess, measure and manage the conduct of business risks associated with its insurance business to ensure the ongoing monitoring and consistent delivery of fair outcomes to policyholders;

(c) comply with all relevant legislation relating to confidentiality, privacy, security and retention of data;

(d) comply with any regulatory reporting requirements;

(e) assess its liability under each of its policies, including data pertaining to each risk that is covered by a policy and each outstanding claim in respect of a policy;

(f) adequately categorise, record and report on complaints as required in terms of Rule 18; and

(g) have access to any other relevant data as prescribed by the Authority.

13.4 An insurer must at a minimum, for the purposes of complying with Rule 13.3, have access to the names, identity numbers and contact details of all its policyholders.

13.5 The contact details referred to in rule 13.4 must be as complete as possible, and where available include the mobile number and email address of the policyholder."

POLICYHOLDER AND POLICY DATA CONTENT GUIDELINES

HIGH LEVEL APPROACH

Based on the regulatory requirements set out above, the guiding principle for the transfer of policyholder and policy data is that the data content must be sufficient to enable the insurer to accept and integrate the transferred data into its own core insurance system and construct a complete view of the policy and schedules as included in the contractual policy documentation sent to the policyholder. This, *inter alia,* will provide the insurer:

I. with the name, identity number (including company and other similar registration numbers) and contact details of policyholders;
II. with all policy and risk details to enable the insurer to assess its liability under each policy; and
III. with the information required to properly identify, assess, measure and manage the conduct of business risks associated with its insurance business.

The information under I and II enables an insurer to have direct access to policyholders for communication purposes and to service clients directly fully and effectively. This includes taking over ongoing policy administration and support and receiving, evaluating and settling any claims under the policy.

Insurers will be in a position to assess their liability under the policy and to have access to policyholder data for communication purposes and effectively underwrite the policy based on the information above. It is also necessary to ensure that insurers are able to provide continuous service to policyholders in the event that the outsourced party is unable to fulfil their obligations hence the insurer will be required to “step-in” in such instances.

POLICYHOLDER DETAILS

PERSONAL LINES POLICIES

- Source of the policy sale (for e.g. Broker name)
- Administrator name
- Policyholder full names
- Type of Identification (ID) and number
- Title (for salutation)
- Value Added Tax (VAT) Number (if VAT vendor)
- Telephone numbers (e.g. home / mobile / work)
- E-mail address
- Physical address
- Postal address
- Policyholder demographic information (see Part 2 of this document: Conduct of Business Returns (CBR) Guidelines)
- Distribution channel (see Part 2 of this document: CBR guidelines)
- Occupation (where applicable)

POLICYHOLDER DETAILS

COMMERCIAL LINES POLICIES

- Source of the policy sale (for e.g. Broker name)
- Administrator name
- Policyholder (registered or trading name per policy)
- Policyholder Registration number (company / other where applicable or as determined by the insurer)
- VAT Number (if VAT vendor)
- Telephone number – of insured entity
- E-mail address – of insured entity
- Contact Person – at insured entity
- Contact Person telephone number
- Contact Person e-mail address
- Physical address (Head Office – Main point of contact)
- Postal address
- Distribution channel (to be aligned to commercial CBR)
- Insurer's chosen market segmentation (to be aligned to commercial CBR)
- Standard Industry Classification (SIC)

POLICY AND RISK DETAILS

PERSONAL LINES POLICIES

A) Policy

- Class of insurance at Policy level (Note 1)
- Policy number/s
- Original inception date
- Policy inception date (i.e. effective date of new or renewed policy under reference)
- Policy Status (Current/Lapsed)
- Policy next renewal/review date
- Policy amendment effective date (if and when amended)
- Policy cancellation effective date (if and when cancelled)
- Total Gross Premium payable including VAT
- Currency if not South African Rands (ZAR)
- Payment frequency (annual/monthly etc.)
- Method of payment (insurer collect/broker collect/other)
- Banking details – for all debit order collections (Note 2)
- Last premium payment date (Note 3)
- Debit order strike date
- Cancellation reason (as agreed between individual insurers and binder holders)
- Product name

B) Section

- Class of insurance at Section level as stated at the beginning of each Section in the policy document – mainly for multi-cover types (Note 4)

C) Risk Items (examples provided for a Motor policy for adaptation to other insurance business classes)

- Item type (e.g. Motor vehicle, Trailer, Caravan etc.) (Note 5)
- Item physical address
- Item description (e.g. Vehicle make/Model etc.) (Note 6)
- Item ID (e.g. Registration/Engine/Vehicle Identification Number (VIN)/Serial numbers etc.)
- Item attributes (Note 7)
- Cover type (e.g. Comprehensive, Third Party, if applicable)

- Risk period start
- Cancellation reason
- Original inception date
- Risk period end
- Risk amendment effective date (Note 8)
- Risk cancellation effective date
- Sum insured/Limit
- Premium (at risk level)
- SASRIA - Yes/No (Y/N) and VAT inclusive SASRIA Premium where applicable (Note 9)
- Excesses (only where variable i.e. voluntary or imposed)
- Value-add Product (VAP) - Y/N and VAP type (see Part 2: CBR guidelines – Section 5) (Only if VAP is not a standalone product)

C1) Risk extensions which are not standard:

- Extension description
- Link Risk extension to Risk Item description under C
- Extension start date
- Extension end date
- Extension amendment effective date
- Extension cancellation effective date
- Extension Sum insured/Limit
- Extension Premium
- Extension Excesses (where variable i.e. voluntary or imposed)

C2) Risk limitations, conditions, exclusions and memoranda:

- Description of risk limitation/condition/exclusion/memorandum
- Link limitation etc. to Risk Item under C

POLICY AND RISK DETAILS

COMMERCIAL LINES POLICIES

A) Policy

- Class of insurance at Policy level (Note 1)
- Policy number
- Original inception date
- Product name
- Policy Status (Current/lapsed)
- Policy inception date (i.e. effective date of new or renewed policy under reference)
- Policy next renewal date
- Policy amendment effective date (if and when amended)
- Policy cancellation effective date (if and when cancelled)
- Total Premium (Gross Premium incl. VAT)
- Currency if not ZAR
- Payment frequency (annual/monthly etc.)
- Method of payment (insurer collects/broker collects/other)
- Banking details – for all debit order collections (Note 2)
- Last premium payment date (Note 3)
- Debit order strike date
- Cancellation reason (as agreed between individual insurers and binder holders)

B) Section

- Class of insurance at Section level as stated at the beginning of each Section in the policy document – mainly for multi-cover types (Note 4)

C) Risk Items

- Item type (Note 5)
- Item physical address
- Item description (Note 6)
- Item ID (e.g. registration/serial number)
- Item attributes (Note 7)
- Risk period start
- Risk period end

- Risk item amendment effective date (Note 8)
- Cover type (e.g. Comprehensive, Third Party, if applicable)
- Cancellation reason
- Original inception date
- Risk item cancellation effective date
- Retroactive date/basis of cover (liability classes)
- Sum insured/Limit
- Premium (at risk level)
- SASRIA – Y/N and SASRIA VAT inclusive Premium where applicable (Note 9)
- Excesses (where variable i.e. voluntary or imposed)
- VAP – Y/N and VAP type (see Part 2: CBR guidelines – Section 5) (Only if VAP is not a standalone product)

C1) Risk extensions which are not standard:

- Extension description
- Link Risk extension to Risk Item description under C
- Extension start date
- Extension end date
- Extension amendment effective date
- Extension cancellation effective date
- Extension Sum insured/Limit
- Extension Premium (at risk level)
- Extension Excesses (where variable i.e. voluntary or imposed)

C2) Risk limitations, conditions, exclusions and memoranda:

- Description of risk limitation, condition, exclusion, memorandum
- Link risk limitation etc. to Risk Item under C

NOTES TO POLICYHOLDER AND POLICY DATA CONTENT GUIDELINES

Note 1: Class of insurance at policy level as it appears on the policy document. Whilst this should align to Class of Insurance Business per Schedule 2 in the Insurance Act, this alignment will already be mapped in insurers' own systems.

Note 2: Banking details – Banking details for all debit order collections should be provided by binder holders on an ongoing basis to enable an insurer to take over the

binder functions, including the collection of premiums, should the binder holder ever be unable to fulfil its obligations ("step-in"). The transfer of policyholder banking details is subject to the adequate identification, governance and oversight by all affected parties of, *inter alia*, the requirements to obtain the appropriate mandates from policyholders before using the banking account details, and compliance with relevant Acts and Regulations, such as and in particular, the Protection of Personal Information Act, 2013. In this regard the joint industry data task team are aware that insurers and binder holders are addressing the associated regulatory requirements differently. Affected parties need to engage specifically on this to ensure both compliance with the regulations and appropriate mitigation of all associated risks.

Note 3**:** Last premium payment date – this is to enable an insurer having to "step-in" to know from what month the premium needs to be charged.

However, this "step-in" requirement in relation to transactional premium accounting presents problems. To take over a monthly collection on the strength of its own records, an insurer needs to maintain a transaction-based policyholder account that tracks and transacts all premiums raised and collections received including pro-rata premiums, unpaids, double and triple debits as well as any broker fees charged and outstanding etc. to ensure a completely seamless transition from broker collection to insurer collection. This mirroring of financial transactions is likely to be impractical if not impossible.

One way of simplifying this, is that instead of maintaining a mirrored premium accounting system for this purpose, the party maintaining the policyholder premium accounting ledger must at least send the balance on each policyholder account prior to the next premium being charged as shown in the same file. The outstanding balance plus the new month's premium is then the amount for collection. However, this is complicated for composite policies where under a broker-collect policy a single debit order is raised that would then be replaced by multiple insurer debit orders and in addition for any broker fee. It is also fraught with practical implementation difficulties.

In view of the low likelihood of an insurer ever needing to "step-in", the minimum requirement is that the insurer must have undeniable access to the records of the party that runs the policyholder ledger so that in the event a "step-in" is required, the insurer can obtain all the transactional information making up the carry forward balance for the covers it provides in order to create the necessary brought forward balance in its own ledgers. This process must be documented and viability audited from time to time.

Note 4: Class of insurance at Section level as it appears in the heading of each section of cover in the policy document. Whilst this should align to Sub-class of Insurance Business per Schedule 2 in the Insurance Act, this alignment will already be mapped in insurers' own systems.

Note 5: Item type - First level description of risk item such as for:

- Motor: Motor car, LDV, Trailer, Caravan
- Property: Private residence, Commercial offices, Factory

Note 6: Item description - Second level description of risk item such as for:

- Motor: Make, Model, Year
- Property: Single / Double story; Office type; Factory type

Note 7: Item attribute – this term is used to include any attribute related to a Risk item that is not addressed under Risk type, Risk description or Risk ID. There are many possible inclusions that are either industry generic or insurer specific such as for:

- Vehicle Body type; Colour; Overnight location; Security; Regular driver; Driver age
- Property: Premises type; Roof type; Wall type; Occupancy; Situation
- Personal Accident: Number of lives covered
- Goods in Transit (GIT): Property insured; Means of conveyance; Cover provided
- Public liability: Basis of cover; Cover provided; Territorial limits
- Personal injury: Category of persons; Business hours limitation; Annual earnings

When the five data elements under Risk item (Type, Physical Address, Description, ID, Attributes) are read together they must comprise of all risk specific information as contained in a hard copy policy schedule which is to be integrated into an insurer's own policy management system in terms of regulatory requirements.

Note 8: Risk amendment date – the start date for cover of an item added to a current policy or for any other change to cover terms and conditions. This may or may not include an additional premium and may or may not have a separate end date before the final expiry date of the policy.

Note 9: SASRIA - Y/N and VAT inclusive SASRIA Premium – may, where applicable, be included as a distinct risk item instead of being attached to another risk item.

CLAIMS DATA CONTENT GUIDELINES

REGULATORY PRINCIPLES

The founding regulatory principles for the transfer of Claims data content are contained in the Insurance Regulations and in the PPRs, Chapter 6, Rule 13: Data Management, with specific reference to:

"13.3 An insurer must have an effective data management framework that includes appropriate strategies, policies, systems, processes and controls relating to the processing of any data which enables the insurer at all times to –

(e) assess its liability under each of its policies, including data pertaining to each risk that is covered by a policy and each outstanding claim in respect of a policy;"

The scope of the claims data guideline is not limited to the scope of the PPRs.

HIGH LEVEL APPROACH

The scope for claims data content to be transferred is enormous, comprising of data relating to claims registration, evaluation, administration, settlement and all associated claims supplies and service suppliers, claims service levels and claims costs.

Most of the information required to inform, assess and settle a claim is often held "off-system" in the form of hard copy or in electronic media that may or may not be structured. As such, it is practically impossible for all information about a claim to be transferred to keep an insurer in a position to be able to seamlessly "step-in" and take over claims' administration at a moment's notice.

The approach taken is therefore to target the following key outcomes:

I. To ensure that policyholders are treated fairly both in terms of the identification and recording of each claim/claimant, the status and eventual settlement value of each claim and associated service levels, in particular to:

    a. Identify the policyholder/policy/risk item against which the claim is being made, and
    b. Monitor the status of individual claims – to provide a high-level view of service levels and in particular to record finalised claims.

II. To have accurate, timeous and dependable financial information about each claim in order to facilitate claims cost accounting, reinsurance reporting and recoveries and for actuarial analysis; and

III. To facilitate regulatory and other reporting.

Apart from this, all claims information and data not included in the framework needs to be held in a pre-agreed form and be accessible by insurers and transferable to insurers as and when required and in particular if the need for insurer “step-in” arises. The data access contingency plan must be documented, tested and available for regulatory inspection.

CLAIMS DETAILS

PERSONAL AND COMMERCIAL

(Note: Policyholder and Policy Data Content Guidelines - “PPDG”)

CLAIM FILE INFORMATION

- Claim number (to uniquely identify claim in systems of both outsource supplier/insurer)
- External reference number (if applicable)
- Policy number (to link to policy information in PPDG)
- Risk Item Identifier/Description (to link to Risk item in PPDG)
- Claim status (to be defined to support insurer CBR reporting)
- Reason for the claims status
- Claim type/Peril
- Date reported
- Date of loss
- Description of loss (brief description for reporting)
- Date re-opened (if applicable)

CLAIM FINANCIAL INFORMATION

- Claims Estimate/Own Damage
- Claims Estimate/Third Party
- Claims Estimate/Service Provider expenses
- Currency if not ZAR
- Own Damage Amount and Date Paid (Claims payments)
- Own Damage VAT Amount
- Third Party Damage Amount and Date Paid (Claims payments)
- Third Party Damage VAT Amount
- Service Provider Amount and Date Paid (Service provider payments)
- Service Provider VAT Amount
- Payment banking details
- Claim dates relevant to Claim Financial Information
- Excess Amount
- Recovery Amount and Date received
- Salvage Amount and Date received

- Salvage VAT Amount
- Payee/Payer Name
- Link claim financial to risk item data
- Service Provider Name/s
- Service Provider VAT number
- Service Provider Address
- Third Party Name (as provided)
- Third Party Telephone Number
- Third Party Address (email/postal/physical as provided)
- Third Party Insurer Details
- Third Party Description of Loss (brief description for reporting)
- Date finalised
- Outstanding claims amount

PART 2

GUIDELINES FOR THE TRANSFER OF CBR AND COMPLAINTS DATA

CBR REPORTING REQUIREMENTS: PERSONAL LINES ONLY

REGULATORY PRINCIPLES

The requirements are referenced from the CBR return template for the industry "*CBR 1 of 2019*" on the FSCA's website. This has been confirmed by the FSCA to be the latest version of the template. Insurers and binder holders need to be further guided by any clarity or changes to this template provided by the FSCA from time to time. The FSCA has advised that CBR reporting is only required for Personal lines business at present.

A marked-up version of the template is attached as **Annexure A** for reference purposes. This comprises questions from both the Non-life Policy level (NLP) sheet and the Non-life Other (NLO) sheet/s (separate worksheets for various cover types: Motor; Property; Agriculture etc).

APPROACH

SECTION 1: BUSINESS COMPOSITION (NLP AND NLO), AND SECTION 2: CLAIMS (NLO)

The majority of the detailed underlying information for both NLP and NLO questions is already available for Policyholder, Policy, Risk and Claims data transfer purposes. With this data being transferred daily, an insurer is able to build most of the aggregate values for CBR reporting.

The following information types are not already covered as outlined above:

- Sales channels – sections 1.7 – 1.9 and 1.14 of the CBR; and
- Client demographic information – sections 1.10 – 1.15.

Insurers will be addressing this individually in the compilation of their returns. Whatever the approach/method, this will need to be communicated by individual insurers to their binder holders in order for information in this format to be obtained by binder holders (much of the information is not currently sourced or held by intermediaries or binder holders) and then transferred to insurers to meet their approach to CBR reporting

requirements. For completeness, these two data elements have been added to the Policyholder and Policy and Risk data under reference to this section.

SECTION 2: COMMISSION, BINDER FEES AND OTHER PAYMENTS (NLP)

This information will be known to insurers from their financial records. No further data elements have been identified for transfer.

SECTION 3: ADVERTISING AND MARKETING SPEND (NLP)

The requirement is for binder holders to *"state the total advertising and marketing expenses paid to all other parties in the last reporting period as per the breakdown: Television; Radio; Print media; Social media; Other".*

To the extent that a binder holder incurs such costs on an insurer's behalf, the information needs to be provided to the insurer as-and-when needed for aggregation with the insurers' own spend for reporting purposes (i.e. to align with Regulatory CBR reporting frequencies).

SECTION 4: COMPLAINTS HANDLING (NLP and NLO)

See Complaints section of the guidelines below.

SECTION 5: ADD-ON BENEFITS (NLP only)

The requirement under 5.1 is to state whether the insurer *"offers any of the following benefits as add-on benefits to the policies?"* Various add-on benefits are listed per Annexure A. Under 5.2, the requirement is to *"state the number of policies with the add-on benefits"* per each benefit type.

For add-on benefits offered by the same insurer that underwrites the core policy, these should be addressed as a separate section under the Policy and Risk section of these guidelines.

For add-on benefits for insured products provided by another insurer, under a separate binder agreement, data needs to be separately transferred to that insurer (only) under these guidelines.

Add-on benefits for non-insurance products are not covered under these guidelines.

COMPLAINTS REPORTING REQUIREMENTS: PERSONAL AND COMMERCIAL LINES (WITHIN SCOPE OF THE PPRs)

REGULATORY REQUIREMENTS

Salient sections of Rule 18: Complaints Management of the PPRs (per **Annexure B**) have been referenced together with Section 2 of the Non-life Other question sheet of the CBR.

APPROACH

To provide complete information as required under the PPRs and CBR, updated every 24 hours.

COMPLAINTS DATA ELEMENTS

- Complaint Reference number (to facilitate complaint counts, referencing and reporting)
- The date the complaint was reported
- The date the complaint was finalised
- Complainant Category – per PPR 18.1 Definition, see Annexure B
- Complainant Full name
- Complainant Contact details – to facilitate communication by insurer
- Complainant Policy number (where individual policy as reflected in Policy data guideline)
- Complainant Group Scheme reference (where group policy)
- Complaint category – per PPR 18.3.1(a) to (i), see Annexure B and CBR reporting requirement under CBR NLO Section: 3
- Complaint Brief details
- Complaint Process Status (to be agreed for insurer monitoring and oversight)
- Complaint Decision Status (to be agreed between insurer/binder holder)
- Complaint settlement estimate (per insurer specification should include any envisaged payments as a result of the complaint e.g. further amounts paid under claim against a policy (item (b) under definition of compensation), compensation payments or goodwill payments) if and where applicable.
- Complaint Compensation payment amount if any and details (per PPR 18.8.2(f))
- Complaint Goodwill payment amount if any and details (per PPR 18.8.2(g))
- Complaint Handler name – at binder holder

PART 3

NON-LIFE INSURANCE DATA REQUIREMENTS

DATA GOVERNANCE

INTRODUCTION:

Parts 1 and 2 of this document have focussed on what data needs to be transferred. In order to properly fulfil the objectives of these data requirements it is essential that the data transferred meets the minimum quality standards set out in this Part 3. It is accepted that most organisations will have certain data governance principles embedded as part of their existing processes. These guidelines, therefore, cover the expected minimum standards and are not prescriptive in terms of the "how" and the "what" for organisations to implement. Organisations should, however, map their own arrangements to these general standards to ensure completeness. This mapping should be referred to in due diligence and audits performed between parties in order to evidence appropriate data governance for purposes of regulatory compliance.

WHAT IS MEANT BY DATA GOVERNANCE?

In referring to data governance for purposes of this document, it means an organisational approach to data and information management that is formalised as a set of policies and procedures that encompass the full data management life cycle, from data acquisition to use to disposal. Establishing a comprehensive data governance framework is a regulatory requirement and ensures confidentiality, completeness, accuracy, integrity, security and availability of data. A typical data lifecycle process will include the following data stages:

- Data collection
- Data processing
- Data usage
- Data monitoring
- Data storage
- Data archival

- Data disposal

KEY DATA PRINCIPLES:

The following principles have been defined to guide the implementation of data governance in the non-life insurance industry that is aligned to regulatory requirements, also in order to promote consistency:

1. ***Quality*** – Insurers and binder holders should ensure that data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for its intended purpose.
   - Monitoring of mandatory fields should be conducted periodically against business rules.
   - Data quality monitoring should be done as close as possible to source through system and process checks.
   - If not in a position to appropriately monitor data, insurers should develop a roadmap that will be inclusive of plans and activities that will allow them to mature in data quality monitoring.

2. ***Usability*** – Data should be easy to understand yet comprehensive enough to facilitate informed decisions.
   - Data reports should be clear and concise and should form part of the insurer's business intelligence function.
   - Insurers should incorporate new data specification changes as part of data collection and capturing processes.
   - Insurers should adhere to the data standards and definitions as approved by the FSCA.

3. ***Accessibility*** – Insurers should be able to access all relevant data for the policies they underwrite (both current and historic data) from the binder holders as frequently as required.
   - Data that is maintained by insurers should be easily accessible within reasonable timelines.

- Insurers should adhere to the FSCA minimum requirements for data accessibility.
- Data should be stored in a secured and controlled environment.
- Data security should be maintained at all times, including the transferring of data from one source to another.
- Data should only be used for the purpose it was initially collected for.

4. ***Audit-ability*** – Data management steps should be regularly monitored and evidence of data changes, enhancements, etc. should be maintained. Insurers should only have access to their own data when conducting reviews on their binder holders.
   - Insurers should put in place Information Technology (IT) general controls such as logical access controls, segregation of duties, data change management processes.
   - All data security processes should produce audit log trails.
   - Evidence of processes followed should be maintained.

5. ***Maintenance*** – Insurers and binder holders should have controls in place in respect of Data maintenance. Data deterioration should be regularly reviewed and maintained such that data remains useful in order to achieve business and other operational requirements.
   - Upon identifying data quality issues through periodic data quality monitoring, insurers should implement activities to correct data.
   - Policyholder data should be updated annually and at every interaction with the client as per the regulatory requirement.
   - Data deterioration should be adequately managed in order to ensure usefulness of data.

6. ***Retention*** – Insurers need to adhere to legislation regarding data retention including before purging data from the archive or production environment.
   - Data retention policies and processes should be in line with legislation and reasons for retaining data should be clearly defined.
   - Data retention mechanisms, including offsite data storage solutions, should be secure and controlled.

- When purging data, the data should be adequately disposed of, for example, hard copies should be shredded and backup tapes be formatted such that the information stored cannot be retrieved in any manner.

SUPPORTING IMPLEMENTATION STANDARDS:

In order to achieve the above stated principles, the following supporting standards should be applied:

1. ***Governance and leadership*** – The organisation has a corporate framework for management and accountability of data quality, with a commitment to secure a culture of data quality throughout the organisation.
   - Accountability and responsibility are clearly and formally defined within the organisation and with partners. This includes the definition of key roles in the organisation such as a data steering group, a data officer, data managers and data users.
   - Data quality is covered by corporate risk management arrangements, with regular assessments of the risks relating to the reliability and accuracy of the information produced and used.
   - Data is subject to robust scrutiny by those charged with governance, and there is formal reporting of data quality issues.
   - There is a formal programme of data quality review, aligned to risk and reported formally to those charged with governance.

2. ***Policies and procedures*** – The organisation has appropriate policies and procedures to secure the quality of the data it records and uses for reporting.
   - There is a comprehensive and current data quality statement, policy, or set of policies, in place. This covers data collection, recording, storage, analysis and reporting, and has been implemented in all business areas.
   - Policies and procedures are applied consistently and comprehensively. Mechanisms are in place to monitor compliance and corrective action is taken where necessary.

3. ***Systems and processes*** – The organisation has systems and processes that secure the quality of data as part of its normal business activities.

- A formal set of quality requirements is applied to all data used by the organisation.
- There are processes in place to validate data from third parties.

TERMINOLOGY:

Data: Data is generally defined as *"a set of values of subjects with respect to qualitative or quantitative variables. Data and information or knowledge are often used interchangeably, however data becomes information when it is viewed in context or in post analysis".* In this regard, reference should also be made to Footnote 1 on page 1. Data is collected, measured, reported and analysed, whereupon it can be visualised using graphs or images. Data as a general concept refers to the fact that some existing information or knowledge is represented or coded in a form which is suitable for improved usage or processing. For the purposes of this document, Data includes both structured and unstructured data and is in electronic form. Data includes both Data in use and Data at rest.

Data governance: Data governance is a control that ensures that the data entry by an operations team member or by an automated process meets precise standards, such as a business rule, a data definition and data integrity constraints in the data model. The data governor uses data quality monitoring against data populations to communicate errors in data back to operational team members, or to the technical support team, for corrective action. Data governance is used by organisations to exercise control over processes and methods used by their data stewards and data custodians in order to improve data quality.

Data management: Data management is the development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of an enterprise.

Data management life cycle: Data management life cycle refers to the practice of applying certain policies for effective information management. A typical data lifecycle process will include the following data stages, namely collection, processing, monitoring, storage, archival and disposal.

Data maintenance: Data maintenance describes the ongoing correction and verification of data, or the process of continual improvement and regular checks of data.

Data quality: Data quality ensures clear understanding of the meaning, context, and intent of the data. It includes components such as accessibility, accuracy, consistency, completeness, currency, definition, granularity, integrity, relevancy and timeliness.

Data security: Data security means protecting data, such as a database, from destructive forces and from the unwanted actions of unauthorised users. In this regard, reference is made to all legislative requirements regarding Data security, including the Protection of Personal Information Act and the global General Data Protection Requirements insofar as they affect any Data under these Data Guidelines.

Data at rest: Data at rest generally refers to data stored in any physical or electronic form.

Data in use: Data in use generally refers to data being processed electronically.

124413