Compliance Procedure V5

01.07.2024

COMPLIANCE SERVICES | DATA SERVICES | INTERMEDIARY SERVICES | RISK SERVICES

Empowering the Financial Services Industry.

T +27 11 214 0900 **E** support@astutefse.com **P** PO Box 2958, Sunninghill, 2157 **A** Building 2, Corporate Campus, 74 Waterfall Drive, Waterfall City, Waterfall, 2090
www.astutefse.com

Table of Contents

1. Introduction 3
2. Company Overview 3
3. Definitions 4
4. Roles and Responsibilities 5
4.1. Astute Compliance Officer 5
4.2. Astute Compliance Committee 6
4.3. Intermediary Compliance Officer 6
4.4. Astute System Users 6
4.5. Astute Support 6
5. Regulatory Instruments 7
6. Related Astute Agreements and Documents 7
7. Stakeholders 7
8. Authorisation 8
9. Astute Audit Types 8
9.1. Daily Audit 8
9.2. Mid-Month Audit 9
9.3. Third Party Audit 9
9.4. Monthly Audit 10
9.5. Random Increased Volumes 10
9.6. Discretionary Audits: 10
10. Received Authorisations 11
11. Procedure in the case where client authorisation cannot be provided. 11
12. Escalation, Investigation and Remedy 12
13. Reinstatement of the transgressor 13
14. List of Annexures 13
15. Policy and Administration 14
ANNEXURE "C1" Destruction and/or Return of Information and/or Intellectual Property 15
ANNEXURE "C2" Consent to Obtain Information 16
ANNEXURE "C3" Consent for Voice Recordings 17
ANNEXURE "C4" Consent for Digital Signatures 18
ANNEXURE "C5" Consent for Special Category Astute System Users 19
ANNEXURE "C6" – Daily Audit Template 21
ANNEXURE "C7" Mid-Month Audit Template 21
ANNEXURE "C8" – Monthly Audit Template 23
ANNEXURE "C9" – Revoking Letter Template 24
ANNEXURE "C10" – CONSENT TO OBTAIN INFORMATION REGARDING UNCLAIMED BENEFITS 25
Business Terminology 28

1. Introduction

The purpose of this document is to identify, capture and provide a clear definition of the Astute Compliance Procedures. It also prescribes actions to be taken for different compliance audits that are conducted, namely:

- Daily audits
- Mid-month audits
- Monthly audits
- Third party audits
- Increased volumes audits
- Discretionary audits

This procedure document also fulfills the purpose of providing Astute's internal and external stakeholders with a general overview of the Astute compliance procedure.

2. Company Overview

Astute Financial Services Exchange is an electronic information exchange company, enhancing the movement and integration of data in the financial services industry. Astute FSE was launched in 2000 as a collaborative effort between the major Life Insurers in South Africa. We provide intermediaries with a single point-of-entry to client's investment and insurance portfolio data.

We are trusted by more than 20,000 intermediaries and we are fully integrated into the business systems and processes of many Life Insurers in South Africa, with more than 150 integration points. This allows us to keep in line with our strategic objective of providing a Single View of the client. Our service offering includes integrations into regulatory offices and government departments to detect and prevent fraud, as well as assist our clients in complying with legislative requirements.

Astute Accreditations and Certifications:

Astute has the following certifications and Gold partner accreditations:

- Microsoft Gold Partner
- ISO 27001 Certification
- ISO 27701 Certification

3. Definitions

For purposes of this Compliance Procedure document, the words and phrases that follow shall have the meaning assigned to them in the corresponding description:

3.1. **Astute** - Astute Financial Services Exchange ("Astute") and all its subsidiaries and associated companies**.**

3.2. **Astute System User** – any of the following role players that have been approved by Astute for use of the Astute system, namely an insurance broker; advisor; trustees; underwriter; technical resources; reinsurers; claims; executors; curators and administrators of deceased Estates. All queries/cases from the Astute System User are to be logged by Astute Support then escalated to the compliance department with a case number.

3.3. **Audit Process** - the procedure during which a system user's compliance with the requirement for valid data subject consent is monitored and tested by means of the compliance officer requesting that system user to produce evidence of the required consent.

3.4. **Compliance Officer** - the person responsible for provision of compliance services in Astute.

3.5. **Consent** - any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information as described in the POPI Act no4 2013.

3.6. **Content Provider** - any supplier of financial products information as defined in FAIS and for purposes of this process with whom the Service Provider has or may enter into an agreement similar in all material respects to this process.

3.7. **Daily Audit** – an audit process that runs daily to check for a system user that individually does over 70 successful transactions in a period space of 12 hours.

3.8. **Data Subject** - shall have the meaning ascribed to it in the POPI Act and shall refer to the person to whom Personal Information relates.

3.9. **Digital Consent Audit** – an audit process carried out on an ad hoc basis that checks for the effectiveness and validity of consent provided through digitals channels.

3.10. **Discretionary Audit** – an audit process carried out by Astute, having reserved its right to conduct such audit at its sole discretion, in respect of any system user.

3.11. **Mid-Month Audit** – an audit process that runs daily to check for a system user that individually does over 70 successful transactions in the period space of a calendar month. This audit will automatically be run on the 1st Monday of each new calendar month as well as the 14th day of

each new calendar month.

3.12. **Monthly Audit** – an audit process that runs monthly to check for all Astute system users who have received successful transactions within the last 30 calendar days. A selection of 8% of the Astute system users within SA Corporate Companies as well as Independent Companies and 10% of Astute system users within Namibia is included in this audit. One transaction per selected Astute system user to be audited. If only one transaction has been performed, that transaction will be included in auditing.

3.13. **Operator** - the Service Provider who processes the Personal Information of the Data Subject without coming under the direct authority of the Data Subject, but on an instruction of the Client.

3.14. **Responsible Party** – a public or private body or any other person which alone or in conjunction with others determines the purpose of and means for processing Personal Information for purposes of the Services.

3.15. **Six Months Rule** - under this rule system user who have been sampled will not be sampled again within the next 6 months.

3.16. **Six months suspension rule** – the minimum period of suspension of a system user's access to the Astute Consolidated Client Profile facility because of non-compliance with the Astute Compliance Procedure and as prescribed by the Astute Compliance committee.

3.17. **Transgressor** – an Astute System User who does not have a valid Authorisation.

4. Roles and Responsibilities

For purposes of the effective execution of the aims of this Astute Compliance Procedure document, the following role players shall carry the responsibilities that are assigned in the corresponding descriptions.

4.1. Astute Compliance Officer

Without in any way detracting from the key performance areas agreed between Astute and the Astute Compliance Officer, the Astute Compliance Officer is a functionary contracted to Astute for the performance of the following responsibilities:

4.1.1 Carrying out the function of identification, assessment, advising on, monitoring and reporting on compliance risk to which Astute may from time to time be exposed;

4.1.2 Overseeing issues relating to general compliance and executing all compliance monitoring for purposes of carrying out disciplinary investigations and making appropriate determinations;

4.1.3 Escalation to the FSPs compliance offices for all investigated cases;

4.1.4 Performance of all audits, escalations to the content provider's compliance officer; and

4.1.5 Relaying of relevant and appropriate information to the Astute Compliance Committee.

4.2. Astute Compliance Committee

The Astute Compliance Committee is a standing Committee supporting the Board of Astute and comprised of representatives of Astute and representatives from Content Providers of Astute.

4.2.1. Is constituted by nominated representative of each of the Content Providers, or an individual invited to form part of the Committee.

4.2.2. Assist in and provide input into disciplinary investigations and making appropriate determinations.

4.2.3. Governed by the Astute Compliance Terms of Reference.

4.2.4. Makes decisions on cases and issues raised by the Astute Compliance Officer or other Committee members.

4.3. Intermediary Compliance Officer

4.3.1 Carry out the function that identifies; assesses; advises on; monitors and reports on regulatory compliance risk.

4.3.2 Oversee issues relating to compliance and execute all compliance monitoring for carrying out disciplinary investigations and making appropriate determinations.

4.3.1 Shall investigate and agree on a course of action with the System User for each breached case based on engagement with the Data Subject whose information was unlawfully breached taking into account the rights of such clients in terms of protection of personal information. Provide feedback to the Astute Compliance Officer within seven business days of the escalation notification.

4.3.1 In the absence of the Compliance Officer the system user is responsible for the responsibilities of the Compliance Officer as set out in this paragraph. This is with reference to Section 17 (5) of FAIS act.

4.4. Astute System Users

4.1.1. Regulated by FAIS, which stipulates that Personal Information relating to a Data Subject in respect of financial products must be verified before changes and/or recommendations are made to the aforementioned financial products.

4.1.2. Be in possession of a valid client authorisation for each instance of doing an Astute Consolidated Client Portfolio online download.

4.5. Astute Support

4.5.1. A department offers a Service where queries and issues are logged, tracked and possibly resolved.

5. Regulatory Instruments

Law - common law and any applicable constitution, statute, by-law, proclamation, regulation, rule, notice, treaty, directive, code of practice, charter, judgement or order having force of law may be applicable in the countries of registration, formation or operation of the parties, and any interpretation of any of them by any court or forum of law and include in particular:

5.1 Unit Trusts Control Act No. 54 of 1981 5.2 Stock Exchange Control Act No. 1 of 1985

5.2 Collective Investment Scheme Control Act No. 45 of 2002

5.4 Securities Services Act No. 36 of 2004

5.5 Financial Advisory and Intermediary Services Act No. 37 of 2002

5.6 Long-Term Insurance Act No. 52 of 1998

5.7 Protection of Personal Information Act No. 4 of 2013

6. Related Astute Agreements and Documents

6.1 Astute Intermediary Agreement

6.2 Content Provision Agreement

6.3 Compliance Committee Code of Conduct

6.4 Astute Compliance Committee Terms of Reference

6.5 Astute Client Consent/Authorisation

7. Stakeholders

7.1 Financial intermediaries

7.2 Content Provider Compliance Officers 7.3 Financial Services Conduct Authority (FSCA)

7.4 Data subjects

7.5 Financial Intermediary Assistants

7.6 Content Providers

7.7 Financial Needs Analysis Software Application Providers (FNAs)7.8 Reinsurers

7.9 South African Police Services (SAPS)

7.10 Claims departments

7.11 Administrators of deceased estates

7.12 Curators

7.13 Trustees

7.14 Underwriters

7.15 Forensics Teams

7.16 Technical Resources, Test Accounts

7.17 Astute Staff

7.18 Content Provider Staff

8. Authorisation

The formats listed below are acceptable forms of consenting and are reviewed and approved by the Astute Compliance Department:

8.1 Scanned manual document

8.2 Voice Consent

8.3 Digital Consent

8.4 Special category users consent

9. Astute Audit Types

9.1. Daily Audit

9.1.1 Audit is executed each day of the year, including weekends and public holidays.

9.1.2 Include all Astute system users i.e. Test users and Astute employees.

9.1.3 All Astute system users (including their assistants) who have received more than the threshold of 70 successful transactions and where the data subject is not found in the previous day.

9.1.4 Two transactions are randomly selected for the audit. The Astute system user may be selected every day if he/she meets the above selection criteria.

9.1.5 The six-month rule does not apply.

9.1.6 Automated system generated email is sent to the Astute system user that has met the set-out criteria and to the Compliance Officer at 08:00 AM each morning (see annexure C6).

9.1.7 The mail includes the details of each transaction that was selected, including the Data Subject, Astute system user and assistant details.

9.1.8 Further detail included in the email: the username, initials, and surname of the Astute system user who submitted the request.

9.1.9 The user is given a maximum of 7 days to send in proof of consent as requested in the letter.

9.1.10 A report is generated on Astute Online – Specifying the details of each transaction that was selected for the daily audit.

9.2. Mid-Month Audit

9.2.1 The audit is performed on the 15th day of each new month, excluding the month of January.

9.2.2 Include all Astute system users i.e. Test users and Astute employees.

9.2.3 The six months rule does not apply.

9.3.4 Select 5 (Five) transactions of Astute system users who have received 70+ successful Data Subject's portfolio (also via their assistants) within the last 30 days from one or more CP's for any of the product sectors i.e. Life & Risk, Linked Investment and Unit Trust.

9.3.5 Automated system generated email is sent to the Astute system user that has met the set-out criteria and to the Compliance Officer at 08:00 AM (see annexure C7).

9.3.6 A report is generated on Astute Online – Specifying the details of each transaction that was selected for the daily audit.

9.3. Third Party Audit

9.3.1 "For the Individual" report is available to the Data Subject on Astute Online to request downloaded information detail https://aol.astutefse.com/Online/CCP/Individual

9.3.2 If the Data Subject queries the Intermediary who requested and accessed their portfolio, the Data Subject must lodge a formal request/complaint to Astute Compliance to confirm client consent from the requesting Intermediary.

9.3.3 The Astute Compliance Officer willsend an email to the data subject explaining the process of the investigation.

9.4. Monthly Audit

9.4.1 The audit is performed on the 1st Monday of each new month, excluding the month of December.

9.4.2 Include all Astute system users i.e. Test users and Astute employees.

9.4.3 The six-monthly rule applies.

9.4.4 One transaction is randomly selected to be audited.

9.4.5 Automated system generated email is sent to the Astute system user and to the Compliance Officer at 08:00 AM (See Annexure C8).

9.4.6 The mail includes the details of each transaction that was selected, including the Data Subject, Astute system user and assistant details.

9.4.7 Further detail included in the email: the username, initials, and surname of the Astute system user who submitted the request.

9.4.8 The user is given a maximum of 7 days to send in proof of consent as requested in the letter.

A report is generated on Astute Online – Specifying the details of each transaction that was selected for the monthly audit.

9.5. Random Increased Volumes

9.5.1 Audit is executed every three months or at an *ad hoc* basis.

9.5.2 A sample of 3% of the transactions are randomly selected for the audit.

9.5.3 The six-month rule does not apply.

9.5.4 Email is sent to the Astute system user.

9.5.5 The mail includes the details of transactions selected.

9.5.6 Further detail included in the email: the username, initials, and surname of the Astute system user who submitted the request.

9.6. Discretionary Audits:

9.6.1 The audit is performed at the discretion of the Compliance Officer, as and when there is a need or a potential risk.

9.6.2 Include all Astute system users i.e. Test users and Astute employees.

9.6.3 The six-monthly rule does not apply.

9.6.4 Several transactions are audited based on transactions performed.

9.6.5 The mail includes the details of each transaction that was selected, including the Data Subject, Astute system user and assistant details.

9.6.6 Further detail included in the email: the username, initials, and surname of the Astute system user who submitted the request.

9.6.7 The user is given a maximum of 7 days to send in proof of consent as requested in the letter.

10. Received Authorisations

10.1 Authorisations received from Astute System Users are checked by the Compliance Officer: initials; surname; validity date and if the authorisations meet the prescribed Astute standards of authorisations. (Annexure “C2” ; Annexure “C3” Annexure “C4”; Annexure “C5”; Annexure “C10”)

10.2 Confirmed authorisations will be communicated back to the Astute System user via email receipt by the Compliance Officer.

10.3 Third Party authorisation is confirmed by the data subject only.

11. Procedure in the case where client authorisation cannot be provided.

Follow Up Reminders

11.1 Reminder email is to be sent to the System User if the response is not received in three business days: if no response is received in three Business days, the following reminder emails are to be sent to the user.

11.1.1The first reminder is sent after three business days from the initial audit communication.

11.1.2 A second reminder is sent after two business days from the first reminder.

11.1.3 A third reminder is to be sent after 24 hours after the second reminder.

A revoking letter is sent where no response is received after 24 Hours after the third reminder (Annexure C9). The above process is followed by the locking of the user profile. A group can also be locked in instances where there is only a single user under the respective group pending further investigation.

12. Escalation, Investigation and Remedy

In the case where a client authorization cannot be provided to Astute Compliance due to it being missing, having never been obtained or other issues that render the authorization suspect, the following will take place:

12.1.1 The Astute Compliance Officer is to notify the Intermediary Compliance Officer of any breach as soon as possible and shall include copies of the compliance records of the performed investigation. The Intermediary Compliance Officer is to carry out the roles and responsibilities as set out in section 3 of this Compliance Procedure. In the absence of the Intermediary Compliance Officer, the System User is responsible for actioning the responsibilities of the Intermediary Compliance Officer as set out in section 3.3 of this document.

12.1.2 The Astute Compliance Officer is to consider the below circumstance prior to proposing the six months suspension (the six months minimum suspension period was set by the Astute Compliance Committee) to the Intermediary Compliance Officer and the Astute System user (transgressor):

12.1.2.1 First time transgressor

12.1.2.2 Did not amend the consent or try in any form to interfere with the investigation.

12.1.2.3 The nature and seriousness of the transgression

12.1.2.4 A satisfactory explanation is to be provided to Astute compliance officer and the intermediary Compliance Officer by the locked system user.

If the above has been satisfied and all the parties agree to the remedy of a six prescribed suspension period. The suspension period will be calculated from the date the final decision is made.

In the presence of the above A and B circumstances or should one of the parties not agree with the minimum three months suspension period proposed; the party that is in dispute of the motion is to request the matter to be taken to the Astute Compliance Committee in writing. The matter will form part of the agenda item to be discussed at the Compliance Committee meeting. The Compliance Committee shall carry out its investigation and return with a decision within 30 days from notification of the complaint.

If the Compliance Committee, by way of majority vote, agree that the compliance breach, as stated in the Intermediary Agreement by the System User is of such a nature to warrant action against the System User, then the Committee reserves the right to take appropriate action which may include permanent suspension from the Astute System and or any other action that the Committee so decides.

a. **The transgressor report must be uploaded on SharePoint:**

https://astutefseza.sharepoint.com/Astute%20Sharepoint/Governance/Compliance/Forms/AllItems.aspx?viewpath=%2FAstute%20Sharepoint%2FGovernance%2FCompliance%2FForms%2FAllItems%2Easpx&id=%2FAstute%20Sharepoint%2FGovernance%2FCompliance%2FAstute%20Random%20Monthly%20Audits

13. Reinstatement of the transgressor

The transgressor will only be reinstated if the following conditions have been satisfied:

13.1 A written statement/email explaining reasons for the transgression and demonstrate an understanding of consent. (The Intermediary Compliance Officer is to be copied)

13.2 The transgressor must inform the data subject of the transgression in writing.

13.3 Nature of the seriousness of the transgression

13.4 First time transgressor

13.5 Did not amend the consent or try in any form to interfere with the investigation

13.6 The nature and seriousness of the transgression

13.7 A satisfactory explanation is to be provided to Astute compliance officer and the intermediary Compliance Office of the locked system user.

The reinstatement will be at a discretion of the Astute Compliance officer.

The transgressor letter must be uploaded on SharePoint for future reference.

14. List of Annexures

ANNEXURE “C1” - DESTRUCTION/RETURN OF PERSONAL INFORMATION Page 10 of 19

ANNEXURE “C2” – MANUAL CONSENT TO OBTAIN INFORMATION

ANNEXURE “C3”- CONSENT FOR VOICE RECORDINGS

ANNEXURE “C4” - CONSENT FOR DIGITAL SIGNATURES

ANNEXURE “C5” – CONSENT FOR SPECIAL CATEGORY ASTUTE SYSTEM USERS

ANNEXURE “C6” – DAILY AUDIT TEMPLATE

ANNEXURE “C7” – MID MONTH AUDIT TEMPLATE

ANNEXURE “C8” – MONTHLY RANDOM AUDIT TEMPLATE

ANNEXURE “C9” – REVOKING LETTER TEMPLATE

ANNEXURE “C10”- CONSENT TO OBTAIN INFORMATION REGARDING UNCLAIMED BENEFITS

ANNEXURE “C11” – ASTUTE CONSENT LEDGER SERVICES – IMPLIED CONSENT

15. Policy and Administration

Contact details of the person responsible for this policy: Sandile Tshabalala, Executive Finance

Tel: +27 11 214 0900

E-mail: Stshabalala@astutefse.com

ANNEXURE “C1” Destruction and/or Return of Information and/or Intellectual Property

In the event of termination of the Services as contemplated in the Intermediary Agreement, the Parties shall comply with the requirements as contemplated in this Annexure, in respect of the destruction and/or return of the Information and/or Intellectual Property.

1. RETURN AND/OR DESTRUCTION OF INFORMATION AND/OR INTELLECTUAL PROPERTY

Each Party undertakes within 14 (Fourteen) days of termination of the Agreement or as soon as reasonably thereafter, to securely return the Information and/or Intellectual Property belonging to the other Party, and/or upon the written request of the other Party destroy, un-install and/or remove all copies of the aforementioned in its possession and/or control and shall notify the other Party that the same has been completed.

2. TERMINATION OF ACCESS TO SERVICES

The Service Provider shall within 14 (Fourteen) days of termination of this Agreement or as soon as reasonably thereafter, terminate any access to any website and/or the Services and shall delete the Information including Information relating to the employees of any Content Provider or FSP or intermediary, which was obtained through the rendering of the Services.

3. AUDIT TRAILS

The Service Provider will retain an audit trail history for purposes of record keeping as may be required in terms of the Law and/or for performing a due diligence investigation.

ANNEXURE “C2” Consent to Obtain Information

I, _____ (full names), with the following Identity Number

_____, in my personal capacity or, where applicable, in a representative capacity for and on behalf

of _____ with the following Identity number _____(state if not applicable), acknowledge the following:

- Sound and proper financial advice can only be provided with full disclosure of relevant information relating to appropriate personal, including private information for the purposes of determining and advising on my/our financial situation and financial product experience and objectives, in the process of acquiring, servicing or maintaining any financial products, including but not limited to any information relating to or interest in any long-term insurance, unit trust or any other financial products or services, with any long-term insurer, unit trust manager or other financial institution;

My/our interests shall be best served if that information is made available to authorized financial service providers with a legitimate interest in receiving such information for those purposes.
I/we accordingly confirm, for the purposes of providing the said sound and proper financial advice to me/us, that full permission and authority is granted to:

_____ (Name of Authorised Astute System User) of

_____ (Name of Intermediary), to obtain any and all such information via The Financial Services Exchange (Pty) Ltd, trading as Astute, or any other institution providing a mechanism for the transmission of such information.
I/We herewith give consent for the long-term insurer, unit trust manager or other financial institution processing such information to release such information to the said Authorised User via the Service Provider, and I/We confirm that such Authorised User shall be acting on my/our behalf or in my/our interests and I/we waive any right to privacy only for the purposes as stated above.

I/We further acknowledge that this consent to obtain information on my behalf will remain effective and valid for a period of 12 months from date of signature below.

This done and signed at _____ on this _____ day of _____ 20___.

_____
Signature of Data Subject/Legal Guardian

ANNEXURE “C3” Consent for Voice Recordings

Compliance Requirement

The following conditions must be adhered to prior to Approval of Voice Recording as Consent. Below are a list of requirements and the process to Verify and Audit on this form of Consent.

The process to follow would be:

1. The technology medium must be such that the calls cannot be tampered with.

2. The backup system must be such that the voice recording is stored and remain accessible for 5 years after termination of the Data Subject relationship to enable any queries to be answered.

3. The backup must allow the voice recording to be easily retrievable in a format that can be played back and clearly heard for Astute audit purposes.

5. The Data Subject needs to accept that the call is being recorded.

6. The voice recording must clearly identify the Data Subject as well as the advisor to whom the consent is given to obtain the Data Subjects policy information.

7. The Data Subject needs to be identified by supplying: Initials, Full names, Surname and ID number

8. A Data Subject Consent Form needs to be read out to the Data Subject, and they need to accept the Consent by either a "Yes" or "No"

9. The Companies Name and FSP License number should also be read out in the above-mentioned process.

10. The consent that is read out must identify Astute as the mechanism through which the information is obtained. The Astute Consent form can be used as a script.

11. A system description of the process (about 2 pages) that will be used should be presented to the Astute Compliance Department for approval.

12. A sample of the voice recording together with the script that will be used must also be supplied to the Astute Compliance Department.

13. Relevant proof or documentation indicating that the voice recording database/system is tamperproof or accessed controlled.

ANNEXURE “C4” Consent for Digital Signatures

The following conditions should be adhered to prior to implementation of Digital Consent as an approved consent process.

1. A reputable vendor is to be utilised and must show that they are compliant with the rules that regulate electronic signatures for any given transaction under South African law. These include the South African Common Law and The Electronic Communications and Transactions (ECT) Act, as well as relevant legislation and authentication of specific transaction types utilised for the consent process.

   Audit Trails are kept, and the transactions are:

   a. Traceable

   A form of signature, certificate, system authentication and document history are automatically generated. The certificate records the time, login user ID, IP address, document serial number, or barcode for document owners and recipients. Or a similar process

   b. Accountability

   An audit trail should be kept for every access, update, or disclosure of the document, or any part of it. This includes information about when and where the document was accessed, updated or disclosed, and the identity of the user or system performing the task.

   c. Document Storage

2. Signed consent forms need to be accessible and available on request. Historical data and archiving of digital consent approvals must be stored for at least 5 years as per the normal requirements.

3. Provide Astute with the assurance of Secure Signing process.

4. Provide Astute with the authentication process followed.

5. Where entities outside of SA are utilised assurance should be provided that all relevant legislation has been considered. The technology medium must be such that the consents cannot be tampered with.

6. A system description of the digital consent process, security etc. should be presented to the Astute Compliance Department for approval.

7. The audit trail/digitally signed document must be easily retrievable and presented upon audit requests.

8. The Data Subject needs to be identified by supplying: Initials, Full names, Surname and ID number.

9. The Data Subject Consent form utilised in the electronic process must comply with the approved consent letter in Annexure "C2"

10. A sample of the audit trail, as well as the digitally signed document, must be supplied to the Astute Compliance Department.

ANNEXURE "C5" **Consent for Special Category Astute System Users**

Special Category users are users utilizing the CCP service for specifically approved purposes, such as underwriting, risk assessment excluding intermediaries bound to the Intermediary Agreement.
To ensure access control, security and compliance to the various protection of personal information act, these users are included under the monthly auditing as well as the Mid-Month and daily process set out in this document.

Current Special Category users allowed access to the Astute Service:

- Where the user is a Re-insurer
- Where the user is an underwriter (new business)
- Where the user is a claims assessor
- Where the user is a Technical resource and is required to do post-production "bug fixes"
- Where a technical resource internal or external, needs to investigate causes of a problem
- The legal entity which is not a financial planner or an ordinary user and is acting in the best interests of the person whose information is being requested, or is acting of an order of the court
- Executors of Estates acting in the interests of the estate
- Trustees
- Administrator of deceased estates
- Curators
- SAPS, who are in possession of subpoenas for a person or persons
- Astute Staff / Test Accounts

Special Category User Grouping / Type	Type of Consent Acceptable (all duly signed/approved etc.)
Reinsurer	➢ A Data Subject consent (Application form consist of Data Subject consent)
SAPS	➢ An Order of the Court
Claims	➢ Consent granted at policy application stage
Technical Resources, Test Accounts & Astute Staff	➢ Case document
Executors	➢ Executorship certificate issued by the Master of the High Court
Administrator of deceased estates	➢ Attorney's letter/certificate of Appointment issued by a local magistrate
Curators	➢ Curator certificate issued by the Master of the High Court
Trustees	➢ A consent signed by the Trustee
Underwriters	➢ A Data Subject Consent (Completed Application form consist of Data Subject Consent)

Deceased Individual policy Requests

Astute System users will be able to request a deceased data subject's policy information provided the below is in place:

- The Astute system user is under a corporate company registered for VOPD system
- Claims department has verified deceased status via VOPD system
- Claims department has verified family lineage through via VOPD system.
- Independent brokers to request Astute support/compliance for the VOPD download at a cost (Still to be confirmed)
- Signed consent by the individual who is family (Lineage confirmed via VOPD system)
- A system user is responsible to only disclose information to individuals who are authorized to receive it.

ANNEXURE “C6” – Daily Audit Template

Compliance Daily Audit 2024

Dear

The Astute Compliance Committee requires random audits to be performed on users that have acquired policy information via the Astute CCP system. Please refer to the below transactions that has been audited.
This is in accordance with clause 5 and 6 of the Intermediary Online Agreement.
https://aol.astutefse.com/Online/Content/Documents/Legal/Intermediary_Agreement.pdf

The details of the transaction are as follows:

Username:
Client name:
Birth date:
Transaction date:

You are requested to send the client authorisation for this particular transaction within 72 hrs. The audit is in line with our compliance procedure.
https://aol.astutefse.com/Online/Content/Documents/Legal/Compliance_Procedure_document.pdf

Type of Client Consent Acceptable (all duly signed/approved etc).

- Broker/Advisor - Client Consent
- Reinsure - A client consent (Application form consist of client consent)
- SAPS - An order of the court
- Claims - Client Claim
- Technical Resources - Case Document
- Executors - Executorship certificate issued by the Master of the High Court
- Administrator of deceased estates - Attorneys letter/certificate of Appointment issued by the local magistrate
- Curators - Curator, certificate issued by the Master of the High Court
- Trustees - Consent signed by the Trustee
- Underwriters - A client consent (Application form consist of client consent)

This information is to be emailed to compliance@astutefse.com or faxed to: 086 683 2335

Your cooperation and urgent attention to this matter would be appreciated. We thank you for your time in this regard and look forward to being of continued service.

Thank you

The Astute Compliance Officer

0861278883

ANNEXURE “C7” Mid-Month Audit Template

Dear

The Astute Compliance Committee requires random audits to be performed on users that have acquired policy information via the Astute CCP system. Please refer to the below transactions that has been audited.
This is in accordance with clause 5 and 6 of the Intermediary Online Agreement.
https://aol.astutefse.com/Online/Content/Documents/Legal/Intermediary_Agreement.pdf

The details of the transaction are as follows:

Username:
Client name:
Birth date:
Transaction date:

Username:
Client name:
Birth date:
Transaction date:

You are requested to send the client authorisation for this particular transaction within 72 hrs. The audit is in line with our compliance procedure.
https://aol.astutefse.com/Online/Content/Documents/Legal/Compliance_Procedure_document.pdf

Type of Client Consent Acceptable (all duly signed/approved etc).

- Broker/Advisor - Client Consent
- Reinsure - A client consent (Application form consist of client consent)
- SAPS - An order of the court
- Claims - Client Claim
- Technical Resources - Case Document
- Executors - Executorship certificate issued by the Master of the High Court
- Administrator of deceased estates - Attorneys letter/certificate of Appointment issued by the local magistrate
- Curators - Curator, certificate issued by the Master of the High Court
- Trustees - Consent signed by the Trustee
- Underwriters - A client consent (Application form consist of client consent)

This information is to be emailed to compliance@astutefse.com or faxed to: 086 683 2335

Your cooperation and urgent attention to this matter would be appreciated. We thank you for your time in this regard and look forward to being of continued service.

Thank you

The Astute Compliance Officer

0861278883

ANNEXURE “C8” – Monthly Audit Template

Compliance Random Audit reminder 2024

Dear

The Astute Compliance Committee requires random audits to be performed on users that have acquired policy information via the Astute CCP system. Please refer to the below transaction that has been audited.
This is in accordance with clause 5 and 6 of the Intermediary Online Agreement.
https://aol.astutefse.com/Online/Content/Documents/Legal/Intermediary_Agreement.pdf

The details of the transaction are as follows:

Username:
Client name:
Birth date:
Transaction date:

You are requested to send the client authorisation for this particular transaction within 72 hrs. The audit is in line with our compliance procedure.
https://aol.astutefse.com/Online/Content/Documents/Legal/Compliance_Procedure_document.pdf

Type of Client Consent Acceptable (all duly signed/approved etc).

- Broker/Advisor - Client Consent
- Reinsure - A client consent (Application form consist of client consent)
- SAPS - An order of the court
- Claims - Client Claim
- Technical Resources - Case Document
- Executors - Executorship certificate issued by the Master of the High Court
- Administrator of deceased estates - Attorneys letter/certificate of Appointment issued by the local magistrate
- Curators - Curator, certificate issued by the Master of the High Court
- Trustees - Consent signed by the Trustee
- Underwriters - A client consent (Application form consist of client consent)

This information is to be emailed to compliance@astutefse.com or faxed to: 086 683 2335

Your cooperation and urgent attention to this matter would be appreciated. We thank you for your time in this regard and look forward to being of continued service.

Thank you

The Astute Compliance Officer

0861278883

ANNEXURE “C9” – Revoking Letter Template

Revoking Notice Audit 2024

Dear

Your Astute online access has been cancelled due to failure to comply with the Compliance audit. On the you were notified that one of your Astute online transactions was selected as part of our compliance audit. This is in accordance with clause 5 and 6 of the Intermediary Agreement.
https://aol.astutefse.com/online/Content/Documents/Legal/Intermediary_Agreement.pdf

Reminders were sent requesting authorisation for the following transaction/s:

Username:
Client name:
Birth date:
Transaction date:

The Service Provider is entitled to immediately terminate the Service where any reason to question the Consent of a Data Subject; or has the reason to question the good faith of the Client, the authorized User or any person acting for and /or on behalf of the Client; or has any reason to believe that the person does not comply with the definition of a Financial Services Provider

The Astute compliance officer shall refer the matter to the Client’s Compliance Officer for further investigation. The Data Subject will be informed of the breach and the An Astute Compliance Committee will be informed. You will be notified of the outcome of the investigation in 7 working days.

Should you require more information please email compliance@astutefse.com or call 0861 27 888 3

Regards
Astute Compliance Officer

ANNEXURE "C10" – CONSENT TO OBTAIN INFORMATION REGARDING UNCLAIMED BENEFITS

I, _____ (full names), with the following Identity Number

_____, in my personal capacity or, where applicable, in a representative capacity for and on behalf

of _____, with the following Identity Number _____ (state if not applicable), acknowledge and agree to the following:

- That I am requesting data concerning the deceased individual with ID number _____and can confirm that I am related to the Deceased. The purpose for the data request is within the ambit of the policy beneficiary benefit. Sound and proper financial advice can only be provided with full disclosure of relevant information relating to appropriate personal, including private information for the purposes of determining and advising on my/our financial situation;
- I understand that no data will be made available or released to me should the data that is requested not confirm me as a stipulated beneficiary on the policy.

My/our interests shall be best served if that information is made available to authorized financial service providers with a legitimate interest in receiving such information for those purposes.
I/we accordingly confirm, for the purposes of providing the said sound and proper financial advice to me/us, that full permission and authority is granted to:

_____ (Name of Authorised Astute System User) of _____ (Name of Intermediary), to obtain any and all such information via The Financial Services Exchange (Pty) Ltd, trading as Astute, or any other institution providing a mechanism for the transmission of such information.
I/We herewith give consent for the long-term insurer, unit trust manager or other financial institution processing such information to release such information to the said Authorised User via the Service Provider, and I/We confirm that such Authorised User shall be acting on my/our behalf or in my/our interests and I/we waive any right to privacy only for the purposes as stated above.

I/We further acknowledge that this consent to obtain information on my behalf will remain effective and valid for its indented purpose of identifying unclaimed benefits from date of signature below.

This done and signed at _____ on this _____ day of _____ 20___.

_____
Signature of Data Subject/Legal Guardian

ANNEXURE "C11" – ASTUTE CONSENT LEDGER SERVICES: IMPLIED CONSENT

Introduction

The Consent Service provides, both internally and externally, an industry wide and recognized ledger platform to store and retrieve client's consent for different product categories.

The system allows a participant to upload their client's consent into the ledger in bulk or single requests. Currently the system allows for participants with implicit consent to store (upload) and retrieve (query) their client consent.

The Consent Ledger is an Astute hosted central ledger for consent. Details of both existing and expired consent on a data subject will be stored in the Ledger.

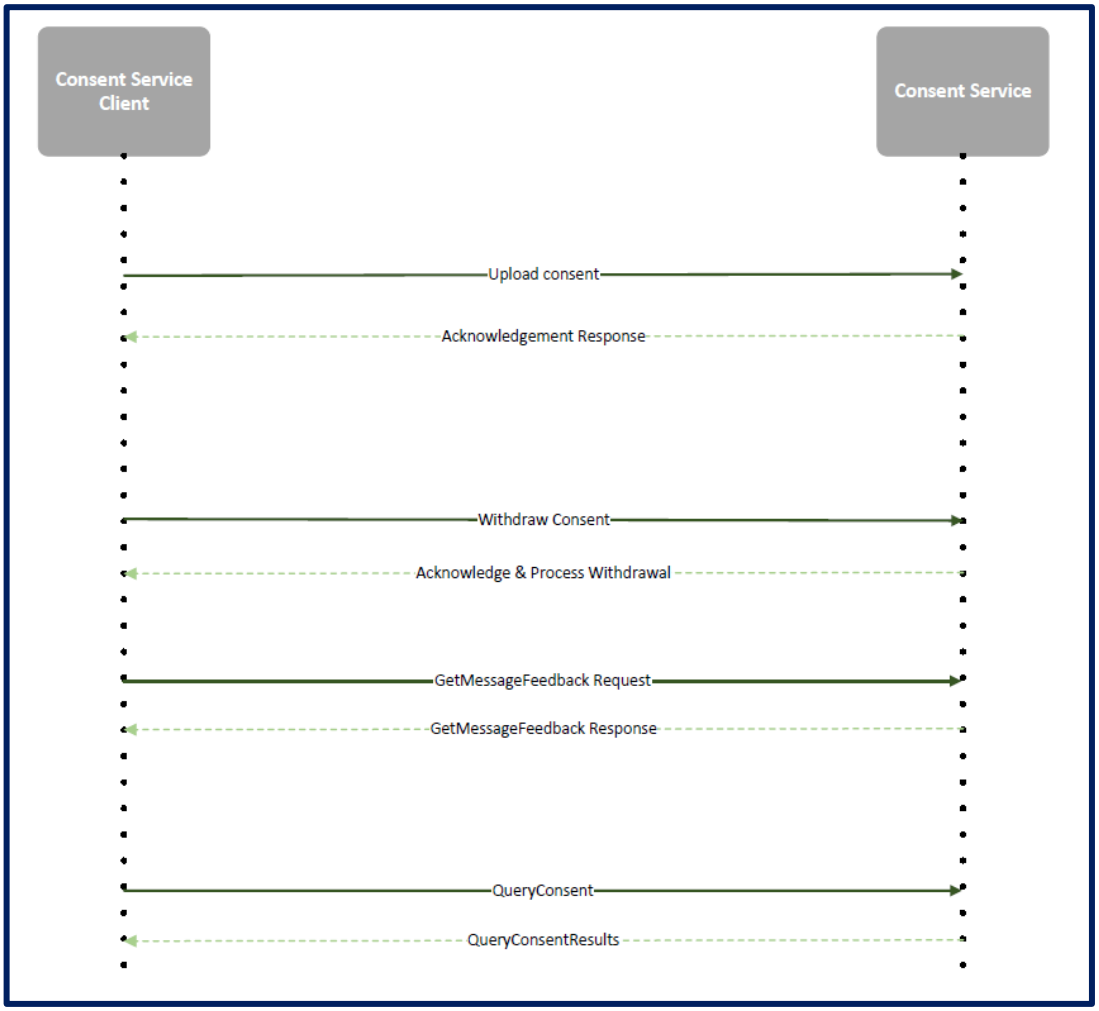
Who is a Data Subject?

Any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity

Information below will be returned to the subscriber

Fields Returned	Data
Consent Requester Code	xxxx
FSP Number	xxxx
Category	1. Financial and Credit Health (Credit Check, Financial Check) 2. Financial Needs Analysis (Life & Risk, Medical, Investment, etc) 3. Risk Management (UW, Claims, Criminal) 4. Statistical Purposes 5. Marketing 6. Comprehensive
Consent Type	Implicit Explicit
ID Type	1. SA ID Number 2. Passport Number 3. Other
DSID Number	xxxxxxxxxxxxxx
Date Consent Approved	YYYY-MM-DD HH:SS
Is Consent Withdrawn	Yes or No / True or False
Date Consent Withdrawn	YYYY-MM-DD HH:SS (if Is Consent Withdrawn = Y)
Authentication Method	1. Two-factor authentication 2. Token authentication 3. Biometric authentication 4. Liveness Check 5. Paper based 6. Face to Face

Fig.1 Consent Service data flow diagram



Business Terminology

Terms	Meaning
Data Subject	Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.
Responsible Party	A responsible party is defined in POPIA as “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information”.
Implicit Consent	Implied consent in this context means consent which is not obtained through the Astute consent service but obtain by the data requester directly from the data subject through other upfront consent and digital identity channels which include data subject authentication.
Explicit Consent	Explicit Consent means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of Personal Information and clearly indicates their choice. Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Explicit consent can be obtained through various means ie electronic forms, emails or the upload of scanned documents with the data subject’s signature (or an electronic signature) by way of examples. What these methods have in common is that there can be a clear trail and explicit consent
Consent Requestor	The party requesting consent to process personal data
Consent Ledger	Astute hosted central industry consent ledger
Consent Combination	Refers to the combination of “Consent Requester Code + Category + Data SubjectID”
Processing	The term “processing” in terms of POPIA has a very wide meaning. It is intended to cover any conceivable operation on data, ranging from collecting, recording and holding, to the subsequent disclosure and eventually destruction of data
Withdrawing Consent	Data Subject has the right to withdraw his/her consent from a responsible party
Disputing Consent	Data Subject has the right to question the consent currently with a responsible party
Field Version Control	Indicate which fields will be a requirement for the corresponding version of Bulk Implicit Consent

Contacts

Service Desk

+27 861 ASTUTE/ +27 86 127 8883
+27 11 214 0903
+27 86 670 0041
support@astutefse.com

Accounts/Finance

+27 11 214 0900
+27 86 670 0041
support@astutefse.com

Compliance

+27 11 214 0918
+27 86 683 2335/ +27 86 686 6121
compliance@astutefse.com

Address

Building 2, Corporate Campus
74 Waterfall Drive,
Waterfall City,
Waterfall, 2090

www.astutefse.com