ACTUARIAL SOCIETY OF SOUTH AFRICA (ASSA)

GENERAL DATA PROTECTION POLICY- APPLICABLE TO ALL REPRESENTATIVES AND SUPPLIERS

1. **DEFINITIONS**

In this Policy:

1.1 "**Consent**" means voluntary, specific, and informed expression of will in terms of which permission is given by a Data Subject for the processing of their Personal Information;

1.2 "**Data Protection Legislation**" means any data protection or data privacy laws applicable to ASSA, including but not limited to POPIA, the Electronic Communications and Transactions Act 26 of 2005, the Promotion of Access to Information Act, 2 of 2000 and the Consumer Protection Act 68 of 2008;

1.3 "**Data Subject**" means an existing and identifiable natural or juristic person to whom Personal Information relates;

1.4 "**ASSA**" or "**We**" means the Actuarial Society of South Africa;

1.5 "**ASSA's Representatives**" or "**Representative** or "**You**" means ASSA's directors, employees, committee members, council members, contractors, agents, officers, representatives, independent contractors, subcontractors, suppliers, licensors, product providers and partners (and their employees), involved in the Processing of Personal Information and similar activities;

1.6 "**Personal Information**" shall have the meaning given to it in terms of any Data Protection Legislation;

1.7 "**Processing**" shall have the meaning given to it in terms of any Data Protection Legislation;

1.8 "**Policy**" means this General Data Protection Policy together with any guidelines or annexes that form part of it;

1.9 "**POPIA**" means the Protection of Personal Information Act, 4 of 2013; and

1.10 "**Special Personal Information**" includes (i) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; (ii) the criminal behaviour of a data subject to the extent that such information relates to: (a) the

alleged commission of any offence by a data subject; or (b) any proceedings in relation to any offence allegedly committed by a data subject or the disposal of such proceedings.

2. PURPOSE OF THIS POLICY

2.1 ASSA is required to comply with applicable Data Protection Legislation, and ASSA can only achieve this if its Representatives, comply with the provisions of this Policy.

2.2 The purpose of this Policy is to assist ASSA's Representatives to comply with Data Protection Legislation whenever they act on behalf of ASSA.

2.3 ASSA and every ASSA Representative will be required to conduct themselves in accordance with this Policy. Accordingly, where ASSA is required to do something under this Policy, the Representative must also act in accordance with that requirement. Similarly, where a Representative is required to do something under this Policy, it is due to ASSA also being required to act in a certain manner in terms of applicable Data Protection Legislation.

3. PERSONS AFFECTED BY THIS POLICY

3.1 This Policy applies to ASSA and, in turn, ASSA's Representatives (as well as all other persons acting on behalf of ASSA) who will be required to conduct themselves in accordance with this Policy.

3.2 It is important that every Representative is familiar with this Policy and implements its provisions in the day-to-day performance of their duties and business dealings. Ignorance of the law is no excuse; accordingly, Representatives must ensure that they have sufficient knowledge of Data Protection Legislation to make educated and informed decisions. In situations where a Representative is unsure as to the correct conduct to follow, they must seek advice from the Information Officer who may, in turn, seek appropriate legal advice where this is necessary.

4. HOW TO USE THIS POLICY

4.1 The Guidelines forming part of this Policy are not a complete statement of the relevant principles contained in the Data Protection Legislation. Accordingly, where there is even the slightest doubt as to the legality of any course of action or business practice, the Representative must immediately refer the matter to ASSA's Information Officer.

4.2 Any contravention of Data Protection Legislation may have a serious and adverse effect on ASSA as well as the individual concerned. Sanctions include significant fines as well as possible criminal and civil law action. No Representative may act contrary to the provisions of the relevant Data Protection Legislation or authorise others to so act.

5. REVISIONS TO THIS POLICY

This Policy is subject to discretional review by ASSA, if there are material changes to applicable laws or if ASSA wishes to enhance or otherwise amend any aspect of this Policy.

6. RESPONSIBILITIES

6.1 Each Representative must learn:

6.1.1 what actions are specifically required or prohibited by the Data Protection Legislation; and

6.1.2 to recognise areas where Data Protection Legislation problems may arise and seek guidance from their line manager, who may in turn refer matters to ASSA's Information Officer.

6.2 Representatives may be required to undergo training regarding compliance with Data Protection Legislation, if and when required by ASSA. Periodic Data Protection Legislation surveys, audits and reviews may be conducted to ensure and monitor adherence to this Policy.

6.3 The provisions of Data Protection Legislation can be complex, and Representatives are encouraged to seek advice if they have any questions. To this end, ASSA's Information Officer will assist Representatives on matters relating to the interpretation of the relevant Data Protection Legislation.

6.4 Senior management is expected to use all reasonable efforts to ensure awareness of, and compliance with, this Policy. Such reasonable efforts include, but are not limited to, frequent communications with Representatives.

7. REPORTING PROCEDURES

7.1 If a Representatives have been involved in or become aware of any violation of this Policy by another Representative of ASSA, it is the Representative's responsibility to report it to ASSA's Information Officer as soon as possible.

7.2 To the extent possible and practical, ASSA will endeavour to maintain the confidentiality and anonymity of the report. If a Representative fears reprisal, he or she should express this concern at the time of the report. In such circumstances the Representative's identity will be kept confidential.

7.3 Retaliation, retribution, or harassment against any Representative who in good faith reports a violation of this Policy is strictly prohibited and, where applicable, constitutes grounds for disciplinary action, including dismissal.

7.4 In circumstances where a Representative wishes to report a violation anonymously, the Representative should contact General Counsel at generalcounsel@actuarialsociety.org.za

8. TRAINING AND EDUCATION

8.1 Certain Representatives will be required to undergo Data Protection Legislation compliance training, including but not limited to online training.

8.2 It is the responsibility of ASSA's Information Officer to ensure that all new Representatives are made aware of this Policy. Compliance messages, alerts and updates regarding Data Protection Legislation developments will be delivered to Representatives to prevent contraventions of Data Protection Legislation.

9. ASSA'S INFORMATION OFFICER

9.1 ASSA's Information Officer is responsible for ASSA's compliance with applicable Data Protection Legislation.

9.2 The CEO is ASSA's Information Officer. The Information Officer can be contacted using the following contact number and email address: ceo@actuarialsociety.org.za

9.3 ASSA's Information Officer is required to:

9.3.1 administer a comprehensive Data Protection Legislation training programme, including but not limited to workshops, small group seminars, online training, email bulletins and manuals;

9.3.2 administer the training of all relevant Representatives regarding the importance and expectation of compliance: (i) during initial orientation sessions; and (ii) on an ongoing basis;

9.3.3 train senior management, as required, to recognise and address compliance issues;

9.3.4 regularly assess Representatives' knowledge of Data Protection Legislation compliance policies and procedures;

9.3.5 document all training sessions;

9.3.6 administer a comprehensive Data Protection Legislation compliance monitoring programme, which includes the tracking and review of incidents of non- compliance with Data Protection Legislation and the submission of the findings to ASSA’s Operations Board.

9.3.7 monitor and investigate all potential Data Protection Legislation violations and report their findings directly to ASSA's Operations Board;

9.3.8 implement adequate remedial measures to prevent violations of Data Protection Legislation laws and consult with the Representatives and human resources managers responsible for making recommendations regarding disciplinary measures for contraventions of this Policy;

9.3.9 review minutes, agendas, registers, policies, standards, and relevant correspondence as well as the filing structure of documents, whether electronically or manually, to identify and address any unlawful data protection practices or concerns;

9.3.10 confirm that the current technical standards are Data Protection Legislation compliant;

9.3.11 conduct an annual audit of compliance procedures and policy;

9.3.12 attend training with specific reference to developments in Data Protection Legislation; and

9.3.13 undertake any other responsibility as set out elsewhere in this Policy.

10. CONSEQUENCES OF NON-COMPLIANCE

10.1 Although ASSA's Information Officer and management team is responsible for the implementation and monitoring of the adherence to this Policy, each Representative is responsible for his or her own actions and to the extent applicable, for the actions of its employees. The consequences of violating this Policy are serious and may expose ASSA to litigation and fines and result in

harm to its reputation. Violation of certain provisions of applicable Data Protection Legislation constitutes a criminal offence, which may result in imprisonment of the individuals involved.

10.2 Representatives should be aware that if ASSA is found to be in contravention of any Data Protection Legislation, civil claims for damages can be instituted by third parties (individuals or companies) against ASSA to recover any loss or damage suffered by the third parties because of ASSA's unlawful conduct, regardless of whether or not there is intent or negligence.

10.3 ASSA will investigate each reported violation and will take the appropriate action. All Representatives have a responsibility to assist and cooperate in any investigation conducted by ASSA or by the Information Regulator. Representatives are also required to follow the Guidelines provided in this Policy document in the event of being contacted by a regulator with jurisdiction under Data Protection Legislation (a "**Regulator**").

10.4 Any Representative of ASSA found to have consciously engaged in unlawful Processing activities or to be negligent in exercising his or her managerial responsibilities in preventing a violation of the relevant Data Protection Legislation will be subject to disciplinary measures and may in certain cases, face dismissal and/or the immediate termination of the business relationship between the parties.

Annexe A

PERSONAL INFORMATION PROCESSING GUIDELINE

1. INTRODUCTION

1.1 Data Protection Legislation regulates the way "**Personal Information**" may be "**Processed**" by ASSA. The concept of Processing is broad, and includes any operation or activity concerning the collection, receipt, storage, updating, use, distribution, and destruction of Personal Information.

1.2 ASSA is required to ensure that it Processes Personal Information in compliance with the conditions for lawful Processing set out in POPIA, when it Processes Personal Information in South Africa.

1.3 In order to ensure that ASSA fulfils its obligations under applicable Data Protection Legislation, this Policy sets out how ASSA Representatives (and other persons Processing Personal Information on ASSA's behalf) must collect, store, update, destroy and otherwise Process Personal Information.

2. SCOPE

All Representatives are responsible for ensuring that they comply with this Guideline and that they implement appropriate practices, processes, and controls to ensure compliance.

3. PROCESSING PRINCIPLES

3.1 ASSA adheres to the principles relating to the Processing of Personal Information set out in POPIA and other pieces of Data Protection Legislation, which require that Personal Information is:

3.1.1 Processed lawfully, in a reasonable manner, and if given the purpose for which it is Processed, it is adequate, relevant, and not excessive (**Processing limitation**);

3.1.2 collected with the Data Subject's knowledge of the purpose for which their Personal Information is collected (**Purpose Specification**);

3.1.3 Processed in a manner compatible with the purpose for which it was originally collected (**Further Processing Limitation**);

3.1.4 complete, accurate, not misleading and updated where necessary (**Information Quality**);

3.1.5 not Processed in a manner that is obscured from the Data Subject (**Openness**);

3.1.6 protected by appropriate and reasonable technical and organisational security measures (**Security Safeguards**); and

3.1.7 accessible to the Data Subject (**Data Subject participation**).

3.2 ASSA is responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

3.3 Accordingly, all Representatives must ensure that they adhere to the principles of lawful processing contained in POPI.

4. PROCESSING LIMITATION

4.1 Data Protection Legislation restricts the way a person may Process Personal Information. Processing must be adequate, relevant, and not excessive given the purpose for which the Personal Information is Processed. These restrictions are not intended to prevent Processing, but to ensure that we Process Personal Information lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject.

4.2 Data Protection Legislation allows Processing under specific circumstances, some of which are set out below:

4.2.1 the Data Subject consents to the Processing;

4.2.2 Processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;

4.2.3 Processing complies with an obligation imposed by law on the Responsible Party;

4.2.4 Processing protects a legitimate interest of the Data Subject;

4.2.5 Processing is necessary for the proper performance of a public law duty by a public body; and

4.2.6 Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied.

4.3 ASSA and its Representatives must identify and document the legal ground being relied on for each Processing activity.

4.4 A Representative may only Process Personal Information when performing his or her job, prescribed duties or in delivering services. A Representative cannot Process Personal Information for any reason unrelated to his or her job, prescribed duties or in delivering services.

4.5 A Representative may only collect Personal Information that is adequate and relevant for the purpose for which the collection is intended and as it is required for the fulfilment of their job, prescribed duties or in delivering services - excessive data should not be collected.

4.6 Representatives must ensure that when Personal Information is no longer needed for specified purposes, it is deleted or anonymised in accordance with ASSA's data retention guidelines (described in more detail below).

4.7 A Data Subject consents to the Processing of their Personal Information if they indicate agreement either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are likely to be insufficient.

4.8 Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if a Representative intends to Process Personal Information for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

4.9 Consent will need to evidenced and captured. Records of all consents (both given and withdrawn by a Data Subject) must be kept so that ASSA can demonstrate compliance with consent requirements.

4.10 Before Special Personal Information or the Personal Information of a child is processed, a Representative must ensure that he or she can identify the lawful basis for Processing such information. For example, Processing of Special Personal Information can take place if:

4.10.1 Processing is carried out with the consent of a Data Subject;

4.10.2 Processing is necessary for the establishment, exercise, or defence of a right or obligation in law;

4.10.3 Processing is necessary to comply with an obligation of international public law;

4.10.4 Processing is for historical, statistical or research purposes to the extent that:

4.10.4.1 the purpose serves a public interest and the Processing is necessary for the purpose concerned; or

4.10.4.2 it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided for to ensure that the Processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

4.10.5 information has deliberately been made public by the Data Subject or a competent person; or

4.10.6 the specific authorisation requirements set out in applicable Data Protection Legislation are complied with if the information relates to a Data Subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal behaviour, or biometric information.

5. PURPOSE SPECIFICATION

5.1 ASSA may only collect, store, update, destroy, or otherwise Process Personal Information for specified purposes. Personal Information must not be further Processed in any manner incompatible with those purposes.

5.2 Representatives will need to ensure that the Data Subject is aware of the purpose for which ASSA is collecting Personal Information.

5.3 Personal Information cannot be used for new, different, or incompatible purposes from those disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and they have consented where necessary.

6. FURTHER PROCESSING LIMITATION

6.1 Where a Representative further Processes Personal Information, he or she must ensure that such further Processing is compatible with the purpose for which it was originally collected.

6.2 To establish whether further Processing is compatible with the purpose of collection, consider:

6.2.1 the nature of the information concerned;

6.2.2 the way the information has been collected; and

6.2.3 any contractual rights and obligations between the Data Subject and ASSA.

7. INFORMATION QUALITY

7.1 Personal Information must be complete, accurate and not misleading, and kept up to date. It must be corrected or deleted without delay, when inaccurate.

7.2 A Representative must ensure that the Personal Information being used and held is accurate, complete, kept up to date and relevant to the purpose for which it was collected. The accuracy of any Personal Information must be checked at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Information.

8. OPENNESS

8.1 ASSA and its Representatives must take reasonably practicable steps to ensure the Data Subject is aware of various matters related to the collection of Personal Information, including, but not limited to:

8.1.1 the type of Personal Information collected the source from which it is collected;

8.1.2 ASSA's details;

8.1.3 the purpose for which the information is collected;

8.1.4 whether the supply of the information is voluntary or mandatory;

8.1.5 the consequences for failing to provide the information;

8.1.6 any law, including Data Protection Legislation, which requires the collection of the Personal Information;

8.1.7 whether ASSA intends to transfer the information to another country and the level of protection afforded to that information in that country;

8.1.8 the recipients of the information;

8.1.9 the Data Subject's right to access, rectify, or object to the collection or Processing of the information;

8.1.10 the right to lodge a complaint with the Information Regulator.

8.2 Whenever Personal Information is collected directly from Data Subjects, including for human resources, membership or employment purposes, ASSA and/or its relevant Representatives must provide the Data Subject with all the aforementioned information. This information must be presented when the Data Subject first provides the Personal Information.

8.3 When Personal Information is collected indirectly (for example, from a third party or publicly available source), the Data Subject must be provided with all the above information as soon as reasonably possible after collecting or receiving the Personal Information. It must also be confirmed that the Personal Information was collected by the third party in accordance with applicable Data Protection Legislation and on a basis which contemplates ASSA's proposed Processing of that Personal Information.

8.4 ASSA must maintain documentation of all Processing operations in sufficient detail to facilitate a request for access to the records of Processing operations.

8.5 Representatives must keep and maintain accurate corporate records reflecting ASSA's Processing, including Records of Data Subjects' consents and procedures for obtaining consents. These Records should include, at a minimum:

8.5.1 the name and contact details of ASSA and the Information Officer;

8.5.2 clear descriptions of:

8.5.2.1 the Personal Information;

8.5.2.2 the Data Subject;

8.5.2.3 the Processing activities;

8.5.2.4 the Processing purposes;

8.5.2.5 third-party recipients of the Personal Information;

8.5.2.6 the Personal Information storage locations;

8.5.2.7 Personal Information transfers;

8.5.2.8 the retention period of the Personal Information (see the Record Retention Guidelines below); and

8.5.2.9 a description of the security measures in place.

8.6 If ASSA has used a Record of Personal Information to decide about a Data Subject, then that Record must be retained:

8.6.1 for such period as may be required or prescribed by law or a code of conduct; or

8.6.2 if there is no law or code of conduct, for a period which will afford the Data Subject a reasonable opportunity to request access to the Record.

9. SECURITY SAFEGUARDS

9.1 Protecting Personal Information

9.1.1 Personal Information must be secured by appropriate and reasonable technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.

9.1.2 ASSA will endeavour to identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control. We will develop, implement, and maintain safeguards appropriate to size, scope and business, available resources, the amount of Personal Information that we own or maintain on behalf of others and identified risks. ASSA will regularly evaluate and test the effectiveness of such safeguards to ensure security of our Processing of Personal Information and update them when new risks are identified. In this regard, it is important that Representatives are responsible for protecting the Personal Information that is Processed by ASSA (to the extent of involvement in the Processing of this Personal Information). Adherence to the security

measures implemented by ASSA against unlawful or unauthorised Processing of Personal Information and against the accidental loss of, or damage to, Personal Information is peremptory. Representatives must exercise particular care in protecting Special Personal Information from loss and unauthorised access, use or disclosure.

9.1.3 All procedures and technologies ASSA puts in place to maintain the security of all Personal Information from the point of collection to the point of destruction must be followed. Representatives may only transfer Personal Information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

9.1.4 Data security must be maintained by protecting the confidentiality and integrity of the Personal Information, bearing in mind that:

9.1.4.1 confidentiality means that only people who have a need to know and are authorised to use the Personal Information can access it; and

9.1.4.2 integrity means that Personal Information is protected against loss, damage, or unauthorised destruction.

9.1.5 Representatives must comply with, and not attempt to circumvent, the administrative, operational, physical, and technical safeguards and standards that ASSA implements and maintains to protect Personal Information.

9.1.6 Anyone who Processes Personal Information on behalf of ASSA is required to Process Personal Information only with ASSA's knowledge or authorisation, and to treat Personal Information which comes to their knowledge as confidential. ASSA is required to conclude a written agreement with everyone who Processes information on our behalf. Please refer any queries You may have in this regard to ASSA's Information Officer.

9.2 **Reporting a Personal Information breach**

You must immediately report to ceo@actuarialsociety.org.za in instances where You suspect that a Personal Information breach has occurred.

10. DATA SUBJECT PARTICIPATION

10.1 Data Subjects have rights when it comes to how ASSA handles their Personal Information. These include, depending on the Data Subject's location, the right to:

10.1.1.1 be notified that Personal Information is being collected;

10.1.1.2 be notified of a Personal Information Breach;

10.1.1.3 access Personal Information held by ASSA;

10.1.1.4 request the correction, destruction, or deletion of Personal Information;

10.1.1.5 object to Processing;

10.1.1.6 restrict our Processing of the Data Subject's Personal Information;

10.1.1.7 object to Direct Marketing;

10.1.1.8 request that ASSA transfer their Personal Information to a third party in an easily accessible format;

10.1.1.9 object to automated decision making; and

10.1.1.10 submit a complaint to the Information Regulator.

10.2 You must verify the identity of an individual making a request under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Information without proper authorisation).

10.3 You must immediately forward any Data Subject request you receive to ASSA's Information Officer.

11. ACCOUNTABILITY

11.1 ASSA is responsible for, and must be able to demonstrate, compliance with the principles of lawful Processing. In this regard, ASSA is required to have adequate resources and controls in place to ensure and to document compliance including:

11.1.1 appointing a suitably qualified Information Officer accountable for data privacy;

11.1.2 integrating the principles of lawful Processing into internal documents including the Policy and related Guidelines;

11.1.3 regularly training ASSA Representatives on Data Protection Legislation, the Policy, related Guidelines, and data protection matters including, for example, Data Subject's rights, consent, the principles of lawful Processing, and Personal Information Breaches. ASSA must maintain a record of training attendance by ASSA Representatives; and

11.1.4 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

11.2 All ASSA Representatives are required to assist ASSA with its efforts in ensuring compliance with Data Protection Legislation, including fulfilling your obligations under this Policy.

12. CHANGES TO THIS GUIDELINE

12.1 ASSA keeps this Guideline under regular review. This version was last updated on **10 May 2022.**

12.2 This Guideline does not override any applicable Data Protection Legislation.

13. Acknowledgement of receipt and review

I, _____, acknowledge that on _____, I received and read a copy of ASSA's Guidelines for Processing Personal Information, and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Guideline is intended to help ASSA Representatives work together effectively on assigned job responsibilities and assist in the use and protection of Personal Information. This Guideline shall form an integral part of the existing relationship in place with the ASSA Representative.

Signed ……..

Printed Name ……..

Date ……..

Annexe B

RECORD RETENTION GUIDELINE

1. INTRODUCTION

1.1 There are legal and regulatory requirements for ASSA to retain certain Records and Personal Information, usually for a specified amount of time. We also retain Records and Personal Information to help our business operate and to have information available when we need it. However, we do not need to retain all Records and Personal Information indefinitely as retaining Records and Personal Information for extended periods of time can expose ASSA to risk as well as be a cost to our business.

1.2 This Guideline explains our requirements to retain Records and Personal Information and to dispose of Records and Personal Information and provides guidance on appropriate data handling and disposal.

2. DEFINITIONS

This Guideline adopts the definitions used in the Policy.

3. SCOPE

3.1 This Guideline covers all Records of Personal Information that ASSA holds or has control over. This includes physical data such as hard copy documents, contracts, notebooks, letters, and invoices. It also includes electronic data such as emails, electronic documents, audio and video Recordings and CCTV Recordings.

3.2 This Guideline covers Records of Personal Information that are held by third parties on our behalf, being Operators, for example, cloud storage providers or offsite Records storage. It also covers Records of Personal Information that belong to us but are held by Representatives on personal devices.

4. GUIDING PRINCIPLES

Through this Guideline, and ASSA's Personal Information retention practices, we aim to meet the following commitments:

4.1 compliance with legal and regulatory requirements to retain Personal Information;

4.2 compliance with our data protection obligations, to keep Personal Information no longer than is necessary for the purposes for which it is Processed (purpose specification principle);

4.3 handling, storage, and disposal of Personal Information responsibly and securely;

4.4 retention of Records only where we need this to operate our association effectively;

4.5 allocation of appropriate resources, roles, and responsibilities to data retention;

4.6 regularly reminding Representatives of their data retention responsibilities; and

4.7 regularly monitoring and auditing compliance with this Guideline and updating this Policy when required.

5. ROLES AND RESPONSIBILITIES

5.1 Responsibility of all ASSA Representatives

ASSA aims to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All Representatives must comply with this Guideline and any communications suspending Record disposal and any specific instructions from the Information Officer. Failure to do so may subject ASSA and its Representatives to serious civil and/or criminal liability. A Representative's failure to comply with this Guideline may result in disciplinary sanctions, including suspension or termination of an applicable contract. It is therefore the responsibility of every Representative to understand and comply with this Guideline.

5.2 ASSA Operations

5.2.1 ASSA's Operations Department is responsible for identifying the Records of Personal Information that We must or should retain and determining the proper period of retention. It also arranges for the proper storage and retrieval of Records, co-ordinating with outside vendors where appropriate. Additionally, ASSA's Records Management Department handles the destruction of Records whose retention period has expired.

5.2.2 The Records Management Officer shall be communicated to ASSA's Representatives from time to time. The Records Management Officer is responsible for:

5.2.2.1 administering the Records management programme;

5.2.2.2 helping department heads implement the Records management programme and related best practices;

5.2.2.3 planning, developing, and prescribing Personal Information and Record disposal policies, systems, standards, and procedures; and

5.2.2.4 providing guidance, training, monitoring and updating in relation to this Retention Guideline.

6. RECORD CLASSIFICATION

6.1 Formal or official information

Certain documents are more important to ASSA and are therefore listed in the Document Retention Schedule. This may be because We have a legal requirement to retain them, or because We may need them as evidence of our transactions, or because it is important to the running of our association. Please see paragraph 7.1 below for more information on retention periods for these types of documents.

6.2 Disposable information

6.2.1 Disposable information consists of information that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not formal or official information. Examples may include:

6.2.1.1 duplicates of originals that have not been annotated;

6.2.1.2 preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official document;

6.2.1.3 books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of ASSA and retained primarily for reference purposes; and

6.2.1.4 spam and junk mail.

6.2.2 Please see paragraph 7.2 below for more information on how to determine retention periods for this type of information.

6.3 **Records of Personal Information**

Both formal or official information and disposable information may contain Personal Information. Data Protection Legislation requires us to retain Records of Personal Information for no longer than is necessary for the purposes for which it was originally collected or subsequently Processed (principle of purpose specification). See paragraph 7.2 below for more information on this.

7. RETENTION PERIODS

7.1 **Formal or official records.**

Any document that is part of any of the categories listed in the Document Retention Schedule must be retained for time indicated in the Document Retention Schedule. A document must not be retained beyond the period indicated in the Document Retention Schedule unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If You are unsure whether to retain a certain Record, contact the Records Management Officer.

7.2 **Records of Personal Information**

7.2.1 As explained above, Data Protection Legislation requires ASSA to retain Records of Personal Information for no longer than is necessary for the purposes for which it was originally collected or subsequently Processed (principle of purpose specification). Where Personal Information is listed in the Document Retention Schedule, ASSA has considered the principle of purpose specification and balanced this against our requirements to retain the Personal Information. Where Personal Information is disposable information, You must consider the principle of purpose specification when deciding whether to retain these Records. More information can be found in the Personal Information Processing Guideline.

7.2.2 Records of Personal Information may be retained if:

7.2.2.1 retention of the Record is required or authorised by law;

7.2.2.2 ASSA reasonably requires the Record for lawful purposes related to our functions or activities;

7.2.2.3 retention of the Record is required by a contract with the Data Subject;

7.2.2.4 the Data Subject has consented to the retention of the Record; or

7.2.2.5 the Records are to be used for historical, statistical or research purposes, provided that appropriate safeguards have been implemented against the Records being used for any other purposes.

7.2.3 If ASSA has used a Record of Personal Information to make a decision about a Data Subject, then that Record must be retained:

7.2.3.1 for such period as may be required or prescribed by law or a code of conduct; or

7.2.3.2 if there is no law or code of conduct, for a period which will afford the Data Subject a reasonable opportunity to request access to the Record.

7.2.4 The period for which Records of Personal Information are to be retained under the above circumstances shall be determined on a case-by-case basis.

7.2.5 You must consult with ASSA's Record Management Department if You are uncertain whether any Record of Personal Information may be retained in under the above circumstances, or the period for which it may be retained.

7.3 **What to do if records are not listed in the Document Retention Schedule.**

If documents are not listed in the Document Retention Schedule, it is likely that it should be classed as disposable information. However, if You consider that there is an omission in the Document Retention Schedule, or if You are unsure, please contact ASSA's Records Management Department.

8. STORAGE, BACK-UP, AND DISPOSAL OF RECORDS

8.1 **Storage**

ASSA documents must be stored in a safe, secure, and accessible manner. Any documents that are essential to our operations during an emergency must

be duplicated and/or backed up at least daily and maintained off site or electronically.

8.2 **Destruction, deletion, or De-Identifying**

8.2.1 The Records Management Officer is responsible for the continuing process of identifying the Records of Personal Information that have met its required retention period and supervising its destruction, deletion, or De-Identification. The destruction of Records of Personal Information must be conducted by shredding if possible. The deletion of electronic data must be co-ordinated with ASSA's IT Department. The destruction or deletion of a Record of Personal Information must be done in a manner that prevents its reconstruction in an intelligible form.

8.2.2 The destruction, deletion or De-Identification of Records must stop immediately upon notification that the Data Subject has requested the restriction of the use of their Personal Information instead.

9. WHERE TO GO FOR ADVICE AND QUESTIONS

Any questions about retention periods relevant to your department should be raised with ASSA's Records Management Department. Any questions about this Guideline should be referred to the Information Officer, who oversees administering, enforcing, and updating this Guideline.

10. BREACH REPORTING AND AUDIT

10.1 **Reporting Guideline breaches**

10.1.1 ASSA is committed to enforcing this Guideline as it applies to all forms of Personal Information. The effectiveness of our efforts, however, depend largely on Representatives. If You feel that You or someone else may have breached this Guideline, you should report the incident immediately to the Information Officer. If You do not report inappropriate conduct, We may not become aware of a possible breach of this Guideline and may not be able to take appropriate corrective action.

10.1.2 No one will be subject to, and we do not allow any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any Record destruction claim, or co-operating in related investigations.

10.2 **Audits**

The Records Management Officer will periodically review this Retention Guideline and its procedures (including where appropriate by taking outside legal or auditor advice) to ensure we follow relevant new or amended laws, regulations, or guidance. Additionally, we will regularly monitor compliance with this Policy, including by carrying out audits.

End