THE AURUM INSTITUTE
DATA PRIVACY POLICY

Policy Information

Policy Status: Approved

Maintained by: Data Management

The signatures below certify that this document has been reviewed and accepted and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensure their provision.

Prepared by	Name	Shanil Batohi	Signature and Date	
	Role	Governance Consultant		
Reviewed by	Name	Marlize Pistorius	Signature and Date	
	Role	Technical Director		
Quality Reviewed by	Name	Jacqueline Paterson	Signature and Date	
	Role	Regional Director: Strategic Information, Data Operations		
Approved by	Name	Dave Clark	Signature and Date	
	Role	Group COO		

TABLE OF CONTENTS

DATA PRIVACY POLICY

INTRODUCTION

1. Data is the lifeblood of any organisation. All transactions and management decisions are based on data. Organisations typically hold vast amounts of data, much of this confidential and organisations often may not be able to function in the absence of this data. It is crucial to correctly manage the integrity, availability and confidentiality of data. With the onset of current global data privacy legislation it is a critical requirement that needs to be met by all organisations operating globally.

SCOPE

2. This policy is relevant to the Aurum Institute Group (the Company), including operations outside of South Africa, including Subsidiaries and Associate/Affiliate companies of the Company.

IMPLEMENTATION OF THE POLICY

3. Related policies, if any exists, that were in force prior to the commencement of this policy are replaced with effect from the date on which an Executive Director approves this policy.

4. This policy applies to all personal data collected, processes or stored at the Company, whether on paper or electronic. This policy does not apply to personal data that is outside the control of the Company, even if the Company has access to this data. This policy also does not apply to data that has been de-identified, with all personal information removed or masked.

PURPOSE OF THE POLICY

5. The purpose of this policy is to detail the mandatory data privacy requirements for the management of all personal information created, processed or stored at the Company.

DEFINITIONS AND ABBREVIATIONS

Definitions

6. **Classification** - Is the process of devising and applying schemes based on the business activities which generate records, whereby they are categorised in systematic and consistent ways to facilitate their capture, retrieval, maintenance and disposal.

7. **Controller** - This is the natural or legal person or persons, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Company is the data controller for any data under the control of the Company.

8. **Data** - Data is raw, unorganised facts that need to be processed. Data can be found in databases, data sets, documents, instant messages, project plans, E-mails, etc. The form in which data is stored could be paper or electronic.

9. **Data Subject** - The person to whom the personal information relates to.

10. **De-identified Data** - This is personal data where all personal content has been removed or masked such that it is not possible to recover the personal content.

11. **Disposal** - Is the process associated with the implementation of appraisal decisions including the retention, deletion or destruction of records.

12. **Documents** - Are sets of recorded information that have not or not yet been assigned corporate value (for example drafts, meeting notes, staff holiday schedules etc.) because they do not need to be kept for legal or regulatory reasons and only have operational value for the company.

13. **Electronic records** - Information which is generated and stored electronically.

14. **General Data Protection Regulation** - The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It

also addresses the transfer of personal data outside the EU and EEA areas.

15. **Information** - Information is data that has been processed, organised, structured or presented in a given context so as to make it more useful.

16. **Personal Data /Information** - Personal information is information such as contact details, age, race, birth date, educational background and employment.

17. **Processor** - This is the natural or legal person or persons, public authority, agency or other body which processes personal data on behalf of the controller. The Company could be the data processor for itself, on behalf of the funder, Department of Health or a partner. A partner could also process The Company's data and would thus be the funder.

18. **Profiling** - This is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

19. **Regulatory Authority** - This is the body in the particular jurisdiction that creates guidelines and regulations, monitors, investigates and enforces the privacy legislation and can allow or disallow exceptions.

20. **Special Categories of Personal Data / Sensitive Personal Informatio**n - This consists of data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Abbreviations

DAMA	Data Management Organisation
DMBOK	Data Management Body of Knowledge 2nd Edition
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
I&T	Information and Technology
ISO	International Organisation for Standardisation
PII	Personal Identifiable Information
POPI	Protection of Personal Information

POLICY STATEMENT

21. This policy deals with the privacy of any personal information collected or held at the Company environment whether paper or in electronic form.

22. Any organisation that has access to or processes personal information held by the Company or on behalf of the Company is also subject to this policy.

POLICY CONTENT

23. Much of the data that is collected and used at the Company is personal information. Personal information is tightly regulated by POPI and other data protection standards. There are also significant penalties for non-adherence and well as reputational risk. This policy states the minimum requirements to be met for the handling of personal information.

24. This policy uses the terms data and information interchangeably.

General

25. **Data Governance Forum:** The Data Governance Forum oversees the implementation of the data privacy requirements.

Data Privacy and Confidentiality

26. **Data Collection Scope**: The Company must ensure that only data that is definitely required for business purposes is collected from external parties. This applies especially to personal information about natural persons. [POPI][GDPR-A5]. The design of systems must be such that only the necessary information is collected [GDPR-A25]. The collection of more sensitive type of personal information (Special Categories of personal information as defined in Definitions Section) is only allowed under exceptional conditions. [GDPR-A9]

27. **Direct Collection**: Personal information must be collected directly from the data subject. [POPI]. For any information not directly collected, the data subject must be informed of this data collection and processing. The following information must be provided to the data subject when the personal data is collected and when an enquiry is made by the data subject [GDPR-A13] [GDPR-A14]:

    27.1. Identity and contact details of responsible person at the Company.

    27.2. The purpose and legal basis for the processing.

    27.3. The legitimate interest pursued by the controller with the processing of this data.

    27.4. The recipients or categories of recipients of the personal data, if the information is transferred outside the Company or outside the country of origin.

    27.5. Whether the personal data is to be transferred to another country.

    27.6. Where the data is not collected directly from the data subject, the data subject must also be informed of what data has been collected.

28. **Consent**: The Company must obtain consent for the collection and specific use of data from the data subject. This consent must be clear and transparent. For personal information of a child under the age of 16 the consent of the parent or legal guardian is required. Consent may only be via Opt-In, not Opt-Out. This consent needs to be stored in a secure manner where the consent can be retrieved if required. [GDPR-A7]

29. **Withdrawal of Consent**: Consent given by a data subject is allowed to be withdrawn and the data subject needs to be informed of their right to withdraw consent. Simple-to-use facilities to enable the withdrawal of consent must be provided. [GDPR-A8]

30. **Data Processing**: Any processing of personal data must be lawful and as agreed with the consent. [GDPR] Only additional processing that is compatible with the original use is allowed without additional consent being obtained. No other use of the data is allowed unless a new consent is obtained for such use. [GDPR-A6][POPI]

31. **Query Personal Information**: A data subject, whether the Company stores or does not store their personal information, has a right to query whether the Company stores their personal information. the Company must be able to respond quickly to any request from any natural person regarding any personal information that they have or do not have in their possession. [GDPR-A15]

32. **Data Erasure**: The data subject can request that the personal data requested be erased, in which case, the data needs to be erased or de-identified unless a legitimate reason for not deleting the data or de-identifying the data exists [GDPR], typically for organisational records or to service the data subject. the Company must ensure that the personal information is either de-identified or destroyed when the information is no longer needed. [POPI] [GDPR-A17]. For research projects this will be dependent on the requirements of the research project as specified

by the funder.

33. **De-Identified Data**: Data that has been de-identified does not need to comply with the privacy requirements in this policy as the person involved cannot be determined.

34. **Data Accuracy**: The Company must attempt to ensure that the data is accurate by means of process or system design. The accuracy of the data must be checked whenever the Company makes contact with the data subject. If the data subject informs the company of any inaccuracy in the data, this must be corrected. [GDPR-A5][POPI]

35. **Data Portability**: The Company must be able to extract personal information for any specific data subject and provide this in a manner suitable for transfer to the data subject or another controller. This must be in the form of a structured, commonly used and machine-readable format. This only applies to data that is under the control of the Company. [GDPR-A20]

36. **Data Integrity and Confidentiality:** Measures must be taken to ensure the integrity of the personal information and to prevent loss, damage or unlawful access to the information. It is required that the internal and external risks are identified, and safeguards be put into place to mitigate these risks. These safeguards must be tested and updated as and when necessary.

37. **3rd Party Privacy Adherence**: If any of the data capturing or processing is outsourced to 3rd parties, then the Company must ensure that the 3rd party meets the data privacy requirements in this policy [POPI] [GDPR-A28] [GDPR-A32]

38. **Data Breach Procedures:** The data subject must be informed of any breach involving their information as soon as possible after the breach has taken place. The relevant regulatory authority and funder/(s) must also be informed of such a breach if the scope of the data collected falls within their jurisdiction. [GDPR-A33] [GDPR-A34] [POPI].

39. **Data Leakage Protection and Detection:** Procedures and automated tools must be implemented to ensure that confidential information is not accidently or deliberately released into the public domain or to unauthorised persons within or outside the company. Procedures need to be put into place to detect any data leakage that takes place. [NIST AC-22][NIST IR-9]

40. **Data Sovereignty**: Personal data must be stored in the country where the person resides or where the data was collected. If this is not possible then the data must be stored only in a country where the privacy laws are compatible with the country in which the data was collected.

41. **Data Transfer:** For the POPI jurisdiction, personal information may not be transferred to a third party in a foreign country. [POPI]. For the GDPR jurisdiction, the transfer of data out of the EU is possible for processing, but the data subject must be informed of this transfer. The processor (and country) needs to meet the GDPR requirements. [GDPR-A44] The conditions under which the transfer of data is possible includes; the country has already been deemed to offer adequate levels of data privacy protection by the relevant supervisory authorities or that the controller and/or processor have offered safeguards and the data privacy laws protect data subjects' rights and are enforceable. [GDPR-A45][GDPR-A46][NIST AC-21]

42. **Automated Processing**: The data subject has a right to not be subject to decisions made purely by automated means. This includes profiling. [GDPR-A22]

43. **Complaints Procedure**: An accessible complaints procedure must be set up and made publicly available. The data subject needs to be made clearly aware of the existence of the objection and complaints process and procedures. [POPI][GDPR-21]

44. **Data Privacy Notices**: Notification of the data subject's rights and remedies must be included in all customer-facing documents or any interfaces in which the data subject enters their personal information. [GDPR-A12]

45. **Demonstrable Compliance**: The Company must implement appropriate technical and company measures to ensure and demonstrate that the processing of personal information is

performed in accordance with GDPR and POPI (where applicable). [GDPR-A24]. A record of all processing of personal information, whether insourced or outsourced, must be kept. [GDPR-A30]

46. **Prior Consultation for High Risk Scenarios**: For data privacy processing that is deemed to be high risk (if the risk mitigation measures were not in place), there must be consultation with the ethics committee, funders and/or regulatory authority before processing starts. [GDPR-A36]

47. **Data on Publicly Accessible Systems**: The integrity of information on a publicly accessible system must be protected to prevent unauthorised access or modification.

48. **Media Outside Company**: Any media that is transferred outside the company's premises needs to be protected by a suitable and predetermined level of encryption. [ISO 8.3.3][NIST AC-3]

49. **Access Protection**: Suitable measures to protect the privacy of personal information as specified in the Records Management Policy must be followed for both paper and electronic personal information.

50. **E-mail Distribution Lists**: Standards and procedures for the setup of E-mail distribution must be compiled. All new distribution lists must be setup by Service Desk only, even though the owner of the distribution list must always be the relevant business unit manager.

CONTRAVENTIONS

51. As contravention of this Policy is a serious matter, it may result in disciplinary action taken in terms of the country Disciplinary Code as promulgated.

RELATED LEGISLATION

52. South African Protection of Personal Information Act No. 4 of 2013 (as amended) and King IV Report on Corporate Governance for South Africa, 2016

53. Primary legislation in Ghana, Data Protection Act, 2012 (Act 843)

54. In Mozambique there is no specific legislation on data protection or privacy. However, the following sources of law impose some privacy obligations:

    54.1. The Civil Code (Decree-Law no. 47344, of November 25, 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967)

    54.2. The Penal Code (Law n.º 35/2014 of December 31)

    54.3. The Labour Law (Law n.º 23/2007, of August 1)

    54.4. The Electronic Transactions Law (Law n.º 3/2017, of January 9)

55. Regulation (EU) 2016/679 (General Data Protection Regulation of 2018)

REFERENCES

56. ISO 27000: Information Security Best Practices

57. DAMA DMBOK Second Edition

58. POL DM 001, Data Management, Annexure A

59. POL DM 002, Data Privacy Policy

60. POL DM 004, Records Management Policy

61. POL ICT 001, IT Security Policy

62. POL ICT 002, End User Policy

REVISION HISTORY

Amendment Record

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual changes, additions or omissions is given below.

Ver #	Approval date	Next Review date	Context	
			Page No.	Significant Changes
1	01/12/2020	12/2022	1-7	First authorised version
2				