

APRIL
2023

POLICY

GROUP PRIVACY POLICY

GROUP-WIDE





CONTENTS

1 INTRODUCTION	3
1.1 PURPOSE	3
1.2 SCOPE AND APPLICATION	3
2 POLICY PRINCIPLES	4
2.1 COLLECTION LIMITATION AND DATA QUALITY	4
2.2 PURPOSE SPECIFICATION	4
2.3 USE LIMITATION	4
2.4 SECURITY SAFEGUARDS	4
2.5 TRANSPARENCY AND OPENNESS	4
2.6 DATA SUBJECT RIGHTS	4
2.7 ACCOUNTABILITY	4
3 OUR APPROACH	5
3.1 DATA LIFECYCLE	5
3.2 COLLECTION	5
3.3 PROCESSING	5
3.4 SHARING	6
3.5 RETENTION	7
3.6 DESTRUCTION	7
4 SECURITY SAFEGUARDS	7
4.1 INFORMATION SECURITY	7
4.2 PRIVACY INCIDENT MANAGEMENT	7
5 TRANSPARENCY AND OPENNESS	8
6 RIGHTS OF DATA SUBJECTS	8
6.1 RIGHT OF ACCESS	8
6.2 RIGHT TO OBJECT	8
6.3 RIGHT OF CORRECTION, DESTRUCTION OR DELETION	8
6.4 RIGHT TO COMPLAIN	8
7 TRAINING	8
8 ACCOUNTABILITY	8
9 ROLES AND RESPONSIBILITIES	9
9.1 DISCOVERY LIMITED BOARD	9
9.2 COMMITTEE OVERSIGHT	9
9.3 INFORMATION OFFICER AND DEPUTY INFORMATION OFFICERS	9
9.4 ATTESTATION	10
10 COMPLIANCE WITH THIS POLICY	10



1 | INTRODUCTION

Discovery Limited and its subsidiaries (“Discovery”) is the custodian of data and information entrusted by its clients, both existing and potential, to it and its subsidiaries. Discovery is committed to ensuring that this data and information are protected in compliance with legislative requirements.

1.1 PURPOSE

The purpose of this policy is to set out the generally accepted principles and approach that apply to the collection, processing, retention, destruction and sharing of personal data and information by Discovery in respect of its clients, potential clients, employees, sub-contractors and other related parties.

The policy is based on global principles which supplement various privacy legislation (Protection of Personal Information Act 4 of 2013 (South Africa), General Data Protection Regulation (EU) 2016/679, UK Data Protection Act (2018), Data Protection (Bailiwick of Guernsey) Law (2017) and jurisdictional and international instruments, but mainly the Core Privacy Principles - The OECD Guidelines (Organisation of Economic Cooperation and Development)).

1.2 SCOPE AND APPLICATION

This policy applies to Discovery and its South African and international subsidiaries. This includes:

- All executive and non-executive directors
- Senior managers
- Full-time, part-time or temporary employees
- Independent contractors or consultants

Each directly held intermediate holding company of Discovery Limited must facilitate the adoption of this Policy by the boards of its directly or indirectly held subsidiaries and is responsible for oversight of adherence to this Policy by its direct and indirect subsidiaries.

As there is no intermediate holding company in respect of the South African domiciled subsidiaries that are directly held by Discovery Limited, the Chief Executive Officer (“CEO”) of SA Inc fulfils the role of oversight and other responsibilities of directly held

intermediate holdings companies as set out in the Policy.

Each subsidiary within Discovery must have processes and procedures in place to align its operations with the spirit and purpose of this Policy. A subsidiary within Discovery may elect to place reliance on the processes and procedures of another subsidiary or to outsource processing of data to another subsidiary or third party. Such reliance must be documented in a written arrangement and any outsourcing must comply with Discovery Outsourcing Policy, where applicable, and include any standard contractual clauses as may be required by Group Legal. The Group Chief Privacy Officer (“GCPO”) and the relevant Compliance function is responsible for providing updates to these standard contractual clauses, as necessary. Despite placing reliance on another subsidiary or outsourcing, accountability for compliance with this policy remains that of the relevant subsidiary within Discovery.

A subsidiary within Discovery may elect to have its own policy considering its nature, scale and complexity, and the legislation under which it operates.

Such a policy must be consistent with this Policy and the Board of Discovery Limited (“Board”) must approve any deviation from this Policy by any of its directly held subsidiaries unless the deviation is necessary to facilitate compliance with legislative and regulatory requirements. In the latter instance, the approval is automatically granted if the board of directors of a subsidiary has communicated the need for such a deviation to the Board.

In respect of indirectly held subsidiaries of Discovery Limited, the board of the relevant intermediate holding company must approve any deviation from this Policy by any of its directly or indirectly held subsidiaries.

The Policy applies to all personal information which Discovery has access to and processes as a Controller or Responsible Party (where that subsidiary determines the means and purposes of processing the personal information) or as an Operator or Processor (where a subsidiary processes personal information under the instruction of a Controller or Responsible Party)



relating to an identified or identifiable data subject or person.

A data subject or person means either a client, potential client, employee, potential employee, third party or any person. A data subject may be an individual or, where applicable, a legal person.

Personal information may be in digital or hardcopy format and may include but is not limited to:

- Names, inclusive of first name, middle name and surname
- Addresses or postal addresses
- Telephone numbers
- Email addresses
- Account information
- Identity or registration numbers
- Special personal information (i.e. information about religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or about the criminal behaviour of a person) Personal telematic information such as data subject's location and drive information

For the purposes of this Policy, processing includes, but is not limited to, any activity concerning personal information, such as: collection, receipt, recording, modification, consultation, storage, distributing, deleting or destroying.

2 | POLICY PRINCIPLES

The personal information processed by Discovery is underpinned by the following 7 principles, which form the foundation of Discovery's approach to privacy:

2.1 COLLECTION LIMITATION AND DATA QUALITY

There should be limits to the collection of personal information and any personal information collected should be obtained by lawful and fair means, where appropriate, with the knowledge or consent of the data subject.

Personal information should be relevant for the purposes for which it is used, and, where necessary

for those purposes, should be accurate, complete and kept up-to-date.

2.2 PURPOSE SPECIFICATION

The purpose for which personal information is collected should be specified.

2.3 USE LIMITATION

Personal information should not be disclosed, made available or otherwise used for purposes other than those for which it was collected, without the consent of the data subject or as required by law.

2.4 SECURITY SAFEGUARDS

Personal information should be protected by reasonable security safeguards against risks such as unauthorised access, destruction, use, modification or disclosure of data.

2.5 TRANSPARENCY AND OPENNESS

There should be a general policy of openness about developments, practices and policies with respect to personal information. A data subject should readily be able to establish the existence and type of personal information, the main purposes of the use of the personal information and the identity of the person responsible for its processing.

2.6 DATA SUBJECT RIGHTS

Individuals should, at a minimum, and where required by applicable data protection legislation, have the right-

- To obtain confirmation of whether or not Discovery has personal information relating to them;
- To receive copies of personal information relating to them; and
- To have their personal information deleted or corrected.

2.7 ACCOUNTABILITY

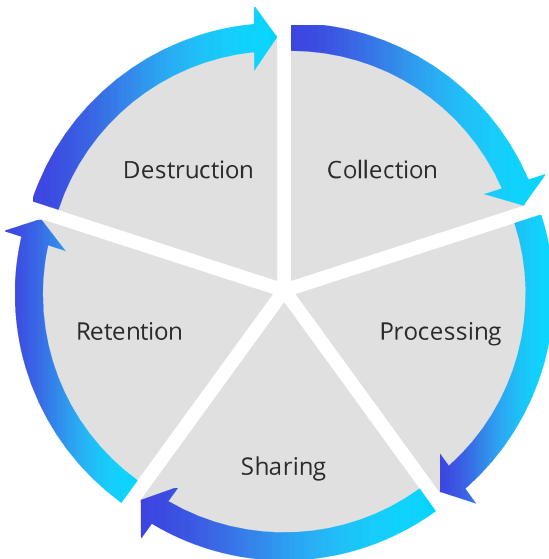
Discovery is accountable for complying with measures to give effect to the above principles and to applicable data protection legislation.



3 | OUR APPROACH

Our approach is linked to the data life cycle as illustrated below. The Policy principles are mapped to the phases of the data lifecycle below:

3.1 DATA LIFECYCLE



3.2 COLLECTION

The amount of personal information collected should be limited only to the personal information required for the purpose for which it is collected. Most importantly, when acting as a Controller or Responsible Party, personal information should be collected from the person themselves where possible and in a lawful manner.

When acting as a Controller or Responsible Party, where the personal information is collected from another source, the person should be informed of this.

When collecting personal information, and when acting as a Controller or Responsible Party, Discovery must ensure that the person is made aware of:

- The details and contact information of the subsidiary which is processing their personal information;
- The type of personal information collected;
- The purpose of the processing;

- Third parties or categories of third parties with whom Discovery shares personal information or who have access to the personal information held by Discovery;
- Their rights; and
- The location where their personal information will be processed, including international transfers and processing.

This disclosure must be clearly contained in a privacy statement which is easily accessible on Discovery's website or the relevant subsidiary's website.

Discovery should only collect personal information from the person if it has a lawful basis for processing the personal information, for example:

- The express, voluntary, informed and specific consent of the person or a competent person where a child is the person;
- A contract between Discovery and the person which requires personal information to be processed;
- A legal obligation; or
- The processing protects a legitimate interest of the person or Discovery.

Discovery, when acting as a Controller or Responsible Party, must ensure that personal information is complete, accurate and not misleading. The information should be appropriate for the purpose for which it was collected.

3.3 PROCESSING

Use Limitation

Personal information must only be processed for the purpose that was stated at the time of collection of the personal information.

If Discovery uses the personal information for any other purpose, then the further processing must be aligned with the original purpose, or the consent of the person must be obtained before any further processing takes place.

Special personal information

Special personal information, otherwise known as sensitive personal information, needs to be treated with specific care, particularly in how it is processed, stored and shared.



Special personal information may only be processed with either the consent of the person or the consent of a competent person in the case where the person is a child, to carry out a legal obligation imposed on Discovery or for statistical or research purposes which are in the public interest. Where applicable legislation provides for additional exceptions, then such exceptions must be considered by the subsidiary concerned.

Children's personal information

Processing of children's personal information without a competent person's consent is prohibited. Similar to special personal information, additional care needs to be taken when collecting, processing and sharing children's personal information.

When personal information relating to a child is processed, it can only be done with the consent of a competent person who is legally entitled to take action or make decisions for the child.

Prior authorisation or regulator approval

Discovery must obtain the prior authorisation of the relevant regulatory authority, where so required by legislation, before collecting and processing the personal information of a child. Prior authorisation need only be obtained once, unless the type or purpose of processing differs on each occasion.

In addition, Discovery must obtain the prior authorisation of the regulatory authority in other instances of processing of personal information, as required by applicable legislation.

Employee personal information

Employees' personal information is to be handled in the same manner as any other person's personal information. It must be processed for the purposes of fulfilling legal obligations and in order to give effect to the employment relationship.

An employee handbook or any other formal document governing the employee relationship must contain details relating to the processing of employee personal information.

Automated processing of personal information

Automated decision making is where a decision is made in the absence of human intervention, and may result in a profile being created about the

person, which is legally binding. This may include a profile of the person's:

- Performance;
- Economic situation;
- Reliability;
- Location;
- Health;
- Personal preferences; or
- Conduct.

A decision based on automated processing may only take place in terms of a contract or as governed by a law or code of conduct. Discovery must allow the data subject the opportunity to express an informed view on and to contest such a decision.

3.4 SHARING

Processing by third parties

Personal information held by Discovery may be processed by third parties such as partners, service providers or other vendors. These relationships must be governed by a written contract which provides for adequate protection of the personal information processed by the third party.

Where a third party has access to or processes the personal information of Discovery clients or employees on Discovery's behalf, Discovery must determine the associated risks before entering into any agreement or sharing any personal information, by conducting a due diligence on the third party.

The person must be informed of the fact that their information is shared, together with the details of the type of third party, for example, a service provider.

Discovery may not disclose personal information to third parties, for purposes other than for processing on behalf of Discovery, unless:

- The consent of the person or competent person where the person is a child, has been obtained; or
- Discovery is under a legal obligation to disclose the information.



Discovery inter-company sharing of personal information

The various South African subsidiaries within Discovery have entered into a Data Sharing Charter (“Charter”). The purpose of the Charter is to allow for the sharing of personal information within the South African strategic strand for purposes of enhancing the quality of services and financial products provided to Discovery clients.

Discovery is to enter into and adhere to the Discovery Group Omnibus Data Transfer Agreement (“Discovery Group ODTA), the purpose of which is to regulate and ensure that personal data processing and transfers, both between various subsidiaries within the same jurisdiction and globally, are adequately safeguarded and lawful.

The Charter is to be repealed once the Discovery Group ODTA has been implemented.

The parties to the Discovery Group ODTA and Charter shall ensure that these documents are adhered to so as to ensure the lawful processing and sharing of personal information.

Cross-border transfer of personal information

Personal information may not be transferred outside of the country in which the information is collected and the responsible Discovery subsidiary is located, unless the recipient is subject to the same or similar legal or contractual requirements relating to the protection of personal information. The transfer of personal information is subject to the relevant legal requirements applicable to the subsidiary concerned.

3.5 RETENTION

Personal information should only be retained for as long as it is required for the original purpose for which it was collected. The legislated retention periods, and in the absence of legislated period, a reasonable retention period at Discovery should be contained in a relevant policy. Exceptions may be made in consultation with the policy owner where:

- An extended retention period is authorised by law;
- Discovery requires the personal information for lawful purposes relating to its functions or activities;

- The personal information is required by a contract between the Controller or Responsible Party and the person; or
- The person, or competent person if the person is a child, has consented to the retention of the personal information.

Personal information collected by the Controller or Responsible Party must be kept up-to-date, accurate and complete for the duration of its retention period.

3.6 DESTRUCTION

Discovery must securely destroy or de-identify personal information that has reached the end of its retention period, and there is no longer a lawful basis, including legitimate interest, to retain the information in accordance with the Data Governance and Data Management Policy.

4 | SECURITY SAFEGUARDS

4.1 INFORMATION SECURITY

Technical and organisational measures must be implemented in accordance with the Group Information Security Policy to ensure the integrity and confidentiality of personal information held by Discovery. These serve to prevent:

- Loss of, damage to or unauthorised destruction of personal information; and
- Unlawful access to or processing of personal information.

4.2 PRIVACY INCIDENT MANAGEMENT

When acting as a Controller or Responsible Party, Discovery is required to report to data subjects and the relevant regulatory authority/ies as soon as reasonably possible or within legislated timeframes, where relevant, when there is an actual unauthorised access, destruction, loss, disclosure or acquisition of personal information and, where applicable, there is a material impact to affected data subject/s.



The Discovery incident handling procedure or similar process document should provide guidance on the handling and response to privacy incidents.

The GCPO is to be informed of privacy incidents which are reportable to the subsidiary's relevant supervisory authority.

5 | **TRANSPARENCY AND OPENNESS**

Discovery must be transparent with relevant persons and regulatory authorities about its practices and policies as it relates to the personal information in its possession.

The information shared with the relevant persons and regulatory authorities must be done in accordance with regulatory requirements.

6 | **RIGHTS OF DATA SUBJECTS**

The below rights shall apply insofar as they arise in terms of the applicable data protection law, to which the person making the request is subject.

6.1 **RIGHT OF ACCESS**

Every person has the right to obtain confirmation that their personal information is held and/or processed by Discovery and to request copies of such personal information.

6.2 **RIGHT TO OBJECT**

All persons have the right to object to Discovery processing their personal information when it is processed on the basis of the person's legitimate interests, for Discovery's legitimate interests or for direct marketing purposes.

Discovery can only refuse if it has compelling and lawful reason to continue processing the personal information.

6.3 **RIGHT OF CORRECTION, DESTRUCTION OR DELETION**

A person has the right to request that their personal information be corrected or deleted if the information is inaccurate, irrelevant, excessive, incomplete, out of date or obtained unlawfully.

A person has the right to request their information be deleted or destroyed if Discovery has retained their information beyond the permissible retention period.

Discovery must notify all persons with whom it shared the incorrect information of the changes made to the information.

6.4 **RIGHT TO COMPLAIN**

A person has the right to submit a complaint to a regulatory authority should they be of the view that Discovery has interfered with the protection of their personal information.

Discovery must ensure that all complaints received are dealt with in accordance with the subsidiary's complaints policy and/or incident handling procedure prior to referring the complainant to the relevant regulatory authority.

7 | **TRAINING**

All persons who are exposed to and process personal information must be trained appropriately in respect of their obligations in terms of this Policy, taking into consideration their roles. Each subsidiary shall ensure that training on this Policy is undertaken. All new employees will be required to complete data privacy training and all employees will be required to complete refresher training annually.

8 | **ACCOUNTABILITY**

Accountability for the lawful processing of personal information by Discovery and its subsidiaries lies with the CEO of each subsidiary or delegated Information Officer, or similar role .



Discovery must have adequate clauses in agreements with operators to ensure that those persons have proportionate technical and organisational measures in place to protect the personal information processed on behalf of Discovery.

The CEO or delegated Information Officer, or similar role must ensure that all employees and directors receive training on data privacy legislation and this policy in order to help them understand their responsibilities when processing personal information.

9 | ROLES AND RESPONSIBILITIES

9.1 DISCOVERY LIMITED BOARD

The Board is the primary custodian of all organisational data and information, as outlined in the Discovery Limited Board Charter. The Board must ensure that Discovery adheres to, and has oversight of, the management of information, to ensure that this results in:

- The ethical and responsible processing of information;
- Sustainability and enhancement of Discovery's intellectual capital through the leveraging of information;
- The protection of privacy of personal information; and
- Compliance with relevant laws.

Discovery Limited has delegated the responsibility of determining the adequacy of systems of controls in managing Discovery's risk and compliance to the Risk and Compliance Committee ("RCC"), as outlined in the RCC Terms of Reference.

The boards of all subsidiaries, where applicable, are responsible for providing assurance to their respective intermediate holding companies that this Policy is implemented.

9.2 COMMITTEE OVERSIGHT

Each subsidiary must mandate a relevant Board committee to exercise oversight on matters relating

to data privacy. This committee will have the responsibility to:

- Review reports published on the status of compliance and risk within Discovery;
- Review any privacy-related matters that could have a significant impact on Discovery's business;
- Consider reports, letters and other communication received from regulatory authorities concerning matters of compliance and management's response thereto;
- Request and consider any other information it deems necessary to verify controls implemented to ensure compliance and risk management controls: and
- Raise matters relating to data privacy with a relevant Board committee.

9.3 INFORMATION OFFICER AND DEPUTY INFORMATION OFFICERS

Each subsidiary within Discovery must appoint, where required by applicable law, in writing, information officer and/or deputy information officer/s or equivalent as defined by global and/or local legislative requirements, such as a data protection officer.

The GCPO is responsible for:

- Acting as the contact point for and co-operating with the regulator, where applicable;
- Providing input into privacy impact assessments carried out by the entities, where required;
- Reporting to the appropriate Group committee; and
- Oversight of and providing steer on Group data protection initiatives.

The GCPO will be supported by deputy information officer/s or equivalent as defined by global and/or local legislative requirements, in each subsidiary.

The responsibilities of such deputy information officer, or equivalent, are as follows:

- The encouragement and monitoring of compliance with applicable data privacy law;
- Dealing with requests under applicable data privacy law;



- Ensuring the privacy risk assessments are carried out relating to the implementation of data privacy legislation; and
- Oversight and providing steer on data protection initiatives as required by applicable data protection legislation.

9.4 ATTESTATION

Each intermediate holding company must provide an annual attestation on the adherence to this Policy including its direct and indirect subsidiaries' adherence facilitated by a Discovery Limited platform.

10 | COMPLIANCE WITH THIS POLICY

Discovery views any non-compliance to this Policy and its obligations in terms of legislation in a serious light.

Compliance with this Policy will be monitored. Any breach of, or non-compliance with this policy must be communicated to the Policy owner as soon as reasonably practical. The Policy owner, with input from key stakeholders, will consider the appropriate action(s) required. All instances of non-compliance with this Policy will be included within the regular risk and compliance reporting processes.



POLICY CONTROL

DETAILS

Policy Owner | Group Chief Privacy Officer

Policy Level | Group Policy

Level of Approval | Board Approval

Frequency of Review | Every second year or if any material legislative or operational changes occur.

REVISION HISTORY

REVISION DATE	VERSION	SUMMARY OF CHANGES	AUTHOR
01 January 2021	Version 1	New Policy	Group Compliance
April 2023	Version 2	Annual review	Group Compliance

POLICY APPROVALS

This policy has been approved as follows:

TITLE	DOCUMENT VERSION	DATE OF APPROVAL
Group Executive Committee	Version 2	19 April 2023
Risk and Compliance Committee	Version 2	24 April 2023
Group Executive Committee	Version 1	7 April 2021
Risk and Compliance Committee	Version 1	21 April 2021

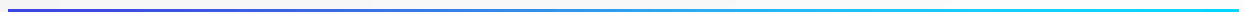
POLICY REFERENCES

This policy should be read together with:

REFERENCE NUMBER	DOCUMENT NAME	DOCUMENT OWNER
1.	Data Governance and Data Management Policy	Group Information Governance and Security
2.	Information Security Policy	Group Information Governance and Security
3.	Cyber Security Incident Response Policy	Group Information Governance and Security
4.	Discovery Group Data Privacy Incident Handling Procedure: Executive Incident Management Team	Group Information Governance and Security



REFERENCE NUMBER	DOCUMENT NAME	DOCUMENT OWNER
5.	Data Sharing Charter (SA Inc)	Group Information Governance and Security
6.	Group Complaints Policy	Group Compliance
7.	Discovery Access to Information Manual	Group Information Governance and Security
8.	Discovery Group Omnibus Data Transfer Agreement	Group Information Governance and Security
9.	USA Privacy and Security Manual	Vitality Group International ISO
10.	Group Data Protection Policy	UK Vitality Data Protection Officer





www.discovery.co.za

Discovery Ltd is the licensed controlling company of the designated Discovery Insurance Group. Registration number: 1999/0077 89/06. Companies in the Group are licensed insurers and authorised financial services providers.

