Viasat

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

Date of Compilation: [10/13/2022]

TABLE OF CONTENTS

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1	**"CEO"**	Chief Executive Officer
1.2	**"Constitution"**	The Constitution of the Republic of South Africa, 1996
1.3	**"DIO"**	Deputy Information Officer
1.4	**"IO"**	Information Officer
1.5	**"Minister"**	Minister of Justice and Correctional Services
1.6	**"PAIA"**	Promotion of Access to Information Act No. 2 of 2000 (as Amended)
1.7	**"POPIA"**	Protection of Personal Information Act No. 4 of 2013
1.8	**"Regulator"**	Information Regulator
1.9	**"Republic"**	Republic of South Africa
1.10	**"Requester"**	In relation to a private body is any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body ***or*** A person acting on behalf of the person contemplated above.

2. INTRODUCTION AND OVERVIEW

This PAIA Manual-

2.1 is published in terms of section 51 of PAIA and gives effect to the provisions of section 32 of the Constitution, which provides for the right of access to information held by another person and that is required for the exercise and / or protection of any rights;

2.2 with reference to any information, in addition to that specifically required in terms of section 51 of PAIA, does not create any right or entitlement (contractual or otherwise) to receive such information, other than in terms of PAIA;

2.3 is for Viasat entities Viasat, Inc., RigNet UK Limited, and Viasat South Africa (PTY) Limited, referred to in this manual as "Viasat." Viasat, Inc. and RigNet UK Limited are foreign companies registered as external companies in South Africa (their registration numbers are 2022/212609/10 and 2014/021507/10, respectively). Viasat provides secure managed communications, machine learning software, digital transformation solutions for connecting and securing complex, remote sites and operational assets in the industries that rely on remote operations in addition to other networking solutions. Viasat is a private body within the definitions of PAIA.

3. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to-

3.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

3.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

3.3 know the description of the records of the body which are available in accordance with any other legislation;

3.4 access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

3.5 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

3.6 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

3.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;

3.8 know the recipients or categories of recipients to whom the personal information may be supplied;

3.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

3.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

4. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF VIASAT

4.1. Chief Information Officer

Name:	Chief Information Officer
Tel:	(844) 702-3199
Email:	privacy@viasat.com
Fax number:	(760) 929-3941

4.2. Deputy Information Officer

Name:	Deputy Information Officer
Tel:	(844) 702-3199
Email:	privacy@viasat.com
Fax number:	(760) 929-3941

4.3 Access to information general contacts

Email:	privacy@viasat.com

4.4 National or Head Office

Postal Address:	6155 El Camino Real Carlsbad, CA 92009 USA
Physical Address:	6155 El Camino Real Carlsbad, CA 92009 USA
Telephone:	(844) 702-3199
Email:	(760) 929-3941
Website:	https://www.viasat.com/

5. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

5.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

5.2. The Guide is available in each of the official languages and in braille.

5.3. The aforesaid Guide contains the description of-

5.3.1. the objects of PAIA and POPIA;

5.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of-

5.3.2.1. every Deputy Information Officer of every private body designated in terms of section 56 of POPIA[1];

5.3.3. the manner and form of a request for-

5.3.3.1. access to a record of a private body contemplated in section 50 of PAIA[2];

---

[1] *Section 56(a) of POPIA- Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.*

[2] *Section 50(1) of PAIA- A requester must be given access to any record of a private body if-*
a) that record is required for the exercise or protection of any rights;

5.3.4. the assistance available from the Regulator in terms of PAIA and POPIA;

5.3.5. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-

5.3.5.1. an internal appeal;

5.3.5.2. a complaint to the Regulator; and

5.3.5.3. a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

5.3.6. the provisions of section 51 of PAIA[3] requiring a private body to compile a manual, and how to obtain access to a manual;

5.3.7. the provisions of section 52 of PAIA[4] providing for the voluntary disclosure of categories of records by a private body, respectively;

5.3.8. the notices issued in terms of section 54 of PAIA[5] regarding fees to be paid in relation to requests for access; and

5.3.9. the regulations made in terms of section 92 of PAIA[6].

5.4. Members of the public can inspect or make copies of the Guide from the offices of private bodies, including the office of the Regulator, during normal working hours.

5.5. The Guide can also be obtained-

5.5.1. upon request to the Information Officer;

---

b) that person complies with the procedural requirements in PAIA relating to a request for access to that record; and
c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

[3] Section 51(1) of PAIA- The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.

[4] Section 52(1) of PAIA- The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access

[5] Section 54(1) of PAIA- The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

[6] Section 92(1) of PAIA provides that –"The Minister may, by notice in the Gazette, make regulations regarding-
(a) any matter which is required or permitted by this Act to be prescribed;
(b) any matter relating to the fees contemplated in sections 22 and 54;
(c) any notice required by this Act;
(d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and
(e) any administrative or procedural matter necessary to give effect to the provisions of this Act."

5.5.2. from the website of the Regulator (https://www.justice.gov.za/inforeg/).

5.6 A copy of the Guide is also available in English, for public inspection during normal office hours

6. VOLUNTARY DISCLOSURE

6.1. Viasat has not published a notice in terms of section 52(2) of PAIA, however, it should be noted that the information relating to Viasat and its services is freely available on Viasat website. Certain other information relating to Viasat is also made available on such website from time to time. Further information in the form of marketing brochures, advertising material and other public communication is made available from time to time.

7. DESCRIPTION OF THE RECORDS OF VIASAT WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

7.1 Information is available in terms of the following legislation to the persons or entities specified in such legislation:

- Companies Act 71 of 2008
- Income Tax Act 58 of 1962
- Value Added Tax Act 89 of 1991
- Tax Administration Act 28 of 201
- Labour Relations Act 66 of 1995
- Basic Conditions of Employment Act 75 of 1997
- Employment Equity Act 55 of 1998
- Skills Development Levies Act 9 of 1999
- Unemployment Insurance Act 30 of 1966
- Regulation of Interception of Communications and Provision of Communication related Information Act 70 of 2002
- Criminal Procedure Act 56 of 1955
- Films and Publications Act 65 of 1996
- Electronic Communications and Transactions Act 25 of 2002
- Occupational Health and Safety Act & Regulations: Act 85 of 1993

Note the above list is not exhaustive and may be amended and/or updated from time to time as the business of the private body evolves.

8. DESCRIPTION OF THE SUBJECTS ON WHICH THE PRIVATE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY VIASAT

8.1. Viasat maintains records on the following categories and subject matters. However, please note that recording a category or subject matter in this PAIA Manual does not imply that a request for access to such records would be honoured. All requests for access will be evaluated on a case by case basis in accordance with the provisions of PAIA.

8.2. Internal records: the following are records pertaining to Viasat's own affairs-

- Memorandum of Incorporation
- Minutes of board or director meetings
- Written resolutions
- Records relating to appointment of directors, auditor, secretary, public officer, or other officers
- Share register and other statutory registers
- Financial records
- Operational records

8.3. Business records: the following are records which have economic value to Viasat-

- Operational records
- Databases
- Published works
- Internal correspondence
- Product records
- Market information
- Marketing and product strategies
- Quality records

8.4. Financial records: the following are records related to the finances of Viasat-

- Financial statements
- Tax returns
- Other documents relating to tax
- Accounting records
- Auditor reports
- Banking records
- Bank statements

- Electronic banking records
- Paid cheques
- Asset register
- Invoices
- Financial agreements
- Management accounts

8.5. Income tax records: the following are records related to Viasat income tax obligations-

- Corporate tax records
- Customs tax
- Documents issued to employees for income tax purposes
- Records of payments made to SARS on behalf of employees
- VAT records
- Regional Services Levies
- Skills Development Levies
- UIF
- Workmen's Compensation

8.6. Insurance records: the following are records related to the insurable assets of Viasat-

- Insurance policies held
- Records of insurance claims
- Register of all immovable property owned by the private body

8.7. Personnel records: the following are records pertaining to any person who works for or provides services to or on behalf of Viasat and receives or is entitled to receive any remuneration and any other person who assists in carrying out or conducting the business of Viasat. This includes, without limitation, directors, executive directors, non-executive directors, all permanent, temporary and part-time staff as well as contract workers. Personnel records include the following-

- Any personal records provided to the private body by their personnel
- Any records a third party has provided to the private body about any of their personnel

- Conditions of employment and other personnel-related contractual and quasi-legal records

- Internal evaluation records
- Other internal records and correspondence

8.8. Policies and directives: both internal and external documents-

- Internal: relating to employees and the private body
- External: relating to customers and other third parties
- Information technology systems and documents

8.9. Agreements or contracts: Both the documents themselves and all related documents-

- Standard agreements
- Contracts concluded with customers
- NDAs
- Letters of intent, MOUs
- Third party contracts (such as JV agreements, VAR agreements, etc.)
- Office management contracts
- Bond agreements
- Rental agreements
- Supplier or service contracts

8.10. Regulatory documents: Any documents Viasat needs to comply with any laws.

- Permits
- Licences
- Authorities

8.11. Customer records: the following customer information-

- Any records a customer has provided to the private body or a third party acting for or on behalf of the private body
- Contractual information
- Customer needs assessments
- Personal records of customers
- Other research conducted in respect of customers
- Any records a third party has provided to the private body about customers
- Confidential, privileged, contractual and quasi-legal records of customers

- Any records a third party has provided to the private body either directly or indirectly
- Records generated by or within the private body pertaining to customers, including transactional records

8.12. Marketing records: the following are records pertaining to other parties, including without limitation contractors, suppliers, joint ventures, service providers and general market conditions. In addition, such other parties may possess records, which can be said to belong to Viasat. The following records fall under this category-

- Market Information
- Public Customer Information
- Product Brochures
- Leads records
- Social media accounts and history
- Performance Records
- Product Sales Records
- Marketing Strategies
- Customer Database
- Sales channel documents

8.13. Other Parties: the following are records pertaining to other parties, including without limitation contractors, suppliers, joint ventures, service providers and general market conditions. In addition, such other parties may possess records, which can be said to belong to Viasat. The following records fall under this category-

- Personnel, customer or the private bodies records which are held by another party as opposed to being held by the private body
- Records held by the private body pertaining to other parties, including financial records, correspondence, contractual records, electronic mail, logs, cached information, records provided by the other party, and records third parties have provided about the contractors/suppliers or customer

8.14. Other Records: Further records are held including-

- Information relating to the private body own commercial activities
- Research carried out on behalf of a client by the private body or commissioned from a third party for a customer
- Research information belonging to the private body, whether carried out itself or commissioned from a third party

Note that the above list is not exhaustive and may be amended from time to time. Accessibility to the above records may be subject to the grounds of refusal as set out in this PAIA Manual. Furthermore, records deemed confidential on the part of a third party, will necessitate permission from the third party concerned, in addition to normal requirements, prior to the private body giving consideration to access.

9. PROCESSING OF PERSONAL INFORMATION

9.1. Purpose of Processing Personal Information

Viasat processes personal information for general business administration purposes, including: (i) to perform contracts; (ii) to comply with legal obligations; (iii) to hire and retain employees; and (iv) otherwise pursue its legitimate interests.

9.2. Description of the categories of Data Subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Personal Information that may be processed
Client Employees	Client employee name and business contact information
Service Provider Employees	Service Provider employee name and business contact information
Viasat Employees	Address, qualifications, training, contact information, information need to administer benefits

9.3. The recipients or categories of recipients to whom the personal information may be supplied

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Client, Employee, and Service Provider business contact information	Service Providers, Clients, and other companies belonging to or affiliated with Viasat Inc.
Employee information	Viasat Inc. and other companies belonging to or affiliated with Viasat Inc.

9.4. **Planned transborder flows of personal information**

Viasat may transfer certain personal information to other companies belonging to Viasat Inc. or entities with which it does business. Where transborder flows of personal information is required Viasat will assure to:

9.4.1. take steps to determine whether you are entitled to transfer personal information about a data subject to a third party in a foreign country; and

9.4.2. confirm that at least one of the additional requirements have been met:

9.4.2.1. the third party is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection of personal information;

9.4.2.2. the data subject consented to the transfer of the personal information to the third party in a foreign country;

9.4.2.3. the transfer is necessary for the performance of a contract between the data subject and your company, or for the implementation of pre-contractual; measures taken in respect of a request by the data subject;

9.4.2.4. the transfer is necessary for the conclusion or performance of a contract concluded between your company and the third party in the interests of the data subject; or

9.4.2.5. the transfer is for the benefit of the data subject, and it is not reasonably practical to obtain the consent of the data subject to that transfer and if it were practical, the data subject would have provided their consent.

9.5. **General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information**

Security measures implemented or to be implemented by Viasat to ensure the confidentiality, integrity and availability for the personal information which may be or is being processed by Viasat under section 51(1)(c)(v) of PAIA. These include the following:

9.5.1. Appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- The pseudonymisation, tokenization, and encryption of “Personal Information”;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Service;
- the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

9.5.2. In addition to above, Viasat undertakes the following specific measures:

9.5.2.1. Access Control of Processing Areas

Suitable measures in order to prevent unauthorized persons from gaining access to the processing equipment (namely telephones, database and application servers and related hardware) where the “Personal Information” are Processed, including:

- establishing security areas;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- logging, monitoring, and tracking all access to the data center where “Personal Information” are hosted; and
- the data center where “Personal Information” are hosted is secured by a security alarm system, and other appropriate security measures.

9.5.2.2. Access Control to Data Processing Systems

Suitable measures to prevent its processing systems from being used by unauthorized persons, including:

- use of encryption technologies per the latest industry standards;
- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;

- automatic temporary lock-out of user terminal if left idle with identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- logging, monitoring, and tracking of all access to data content.

9.5.2.3. Access Control to Use Specific Areas of Data Processing Systems

Ensuring that the persons entitled to use its processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that "Personal Information" cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the "Personal Information";
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the "Personal Information";
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of encryption technologies per the latest industry standards; and
- control of controlled files and documented destruction of data in a timely manner.

9.5.2.4. Availability Control

Suitable measures to ensure that "Personal Information" are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- storage of backup at an alternative site that is available for restore in case of failure of the primary system.

9.5.2.5. Transmission Control

Suitable measures to prevent the “Personal Information” from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This shall be accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- encryption of certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) within the system;
- providing user alert upon incomplete transfer of data (end to end check); and
- logging, monitoring, and tracking of all data transmissions, as far as possible.

9.5.2.6. Input Control

Suitable input control measures, including:

- an authorization policy for the input, reading, alteration, and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration, and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time;
- proof established within data importer/sub-processor’s organization of the input authorization; and
- electronic recording of entries.

9.5.2.7. Separation of Processing for Different Purposes

Suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- through the use of encryption technologies per the latest industry standard;
- modules within the data importer's/Sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;
- with proper documentation specifying the data needed and its intended function;
- at the database level, data is stored in different normalized tables, separated per module, per controller or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is Processed separately.

9.5.2.8. Monitoring

Suitable measures to monitor access restrictions to Vendor's system administrators and to ensure that they act in accordance with instructions received. This shall be accomplished by various measures including:

- individual appointment of all privileged level users;
- adoption of suitable measures to register all privileged users' access logs to the infrastructure and keep them secure, accurate, and unmodified for at least six months; and
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/Sub-processor and applicable laws.

10. GROUNDS FOR REFUSAL

10.1 Viasat reserves the right to refuse you access to certain records in terms of PAIA and POPIA in order to protect:

10.1.1 the privacy of a third party;

10.1.2 the commercial records of a third party in terms of an agreement;

10.1.3 the confidential information in terms of an agreement;

10.1.4 the safety of a person or Juristic person;

10.1.5 information in legal proceedings;

10.1.6 national security;

10.1.7 the intellectual property or trade secrets of the private body; and

10.1.8 frivolous or vexatious, involve an unreasonable diversion of resources

On receipt of a duly completed access request form, we will endeavour to notify you in writing within 30 days as to whether your request has been approved or declined. If we cannot find any requested record and/or where it is determined that no such record exists, we shall formally notify you that it is not possible to provide access to that particular record.

11. ACCESS REQUEST PROCEDURE

11.1 A requester requiring access to information held by a private body must complete the prescribed form or Form 02: Request for Access to Record [Regulation 7 of PAIA] accessible at https://www.justice.gov.za/inforeg/docs/forms/InfoRegSA-PAIA-Form02-Reg7.pdf and submit same to the private bodies Information Officer as per the contact details stated in paragraph 4 above as well as pay the applicable request fees.

11.2 If a request is made on behalf of another person, then the requester must submit proof of the capacity in which the requester is making the request to the reasonable satisfaction of the private bodies Information Officer.

11.3 On receipt of a duly completed access request form, the private body will notify the requester in writing within 30 days as to whether his/her request has been approved or declined. If the private body cannot find any requested record and/or where it is determined that no such record exists, the private body shall formally notify the requester that it is not possible to provide access to that particular record.

12. ACCESS REQUEST FEES

12.1 Section 54 of PAIA provides that the head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request. The requester must contact the private bodies Information Officer for up to date schedule of fees, no information and/or records will be provided to the requester until the requester has paid all outstanding fees in full.

13. COMPLAINTS TO THE INFORMATION REGULATOR AND APPLICATION TO COURT

13.1. The requester may submit a complaint in writing to the Information Regulator, within 180 days of the decision, alleging that the decision was not in compliance with the provisions of PAIA. An application to court may be brought in the ordinary course of business.

14. AVAILABILITY OF THE MANUAL

14.1. A copy of the Manual is available:

14.1.1. on www.viasat.com, if any;

14.1.2. head office of Viasat for public inspection during normal business hours;

14.1.3. to any person upon request and upon the payment of a reasonable prescribed fee; and

14.1.4. to the Information Regulator upon request.

14.2 A fee for a copy of the PAIA Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

15. UPDATING OF THE MANUAL

Viasat will on a regular basis update this manual.

Issued by

Chief Information Officer