SPARK ATM SYSTEMS (PTY) LTD

Registration Number: 2005/030567/07

PROMOTION OF ACCESS TO INFORMATION MANUAL PREPARED IN TERMS OF SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2002

and

THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

Date of Compilation: 7/11/2020

TABLE OF CONTENTS

1. PURPOSE AND DEFINITIONS

1.1 PAIA and POPIA give effect to the constitutional right of access to any information in records held by public or private bodies that is required for the exercise or protection of any rights. PAIA sets out the requisite procedural issues attached to such request, the requirements which such request must meet as well as the grounds for refusal or partial refusal of such request.

1.2 This manual is intended to assist a Requester regarding the procedures to follow in order to request access to information to which the Requester may be entitled in terms of PAIA and POPIA. A Requester has the right to submit a request, after providing adequate proof of identity and after payment of any fee required by law (if applicable) under Annexure "**A**".

1.3 PAIA and POPIA recognise that the right of access to information cannot be unlimited and should be subject to justifiable limitations, including, but not limited to:

1.3.1 limitations aimed at the reasonable protection of privacy;

1.3.2 commercial confidentiality; and

1.3.3 effective, efficient and good governance;

and in a manner which balances that right with any other rights, including such rights contained in the Bill of Rights in the Constitution of the Republic of South Africa, Act 108 of 1996, as amended and POPIA.

1.4 This right of access may not be used to access records under criminal or civil proceedings, or where such proceedings have commenced.

1.5 For the purposes of this manual, unless the context indicates the contrary:

1.5.1 "**Access Fee**" means a variable fee prescribed for the purposes of section 54(6) of PAIA and set out in the attached schedule marked "**A**";

1.5.2 **"Conditions for Lawful Processing"** means the conditions for the lawful processing of Personal Information as fully set out in chapter 3 of POPIA;

1.5.3 **"Data Subject"** has the meaning ascribed thereto in section 1 of POPIA;

1.5.4 "**Head**" means the head of Spark as defined in section 1 of PAIA and referred to in paragraph 2.3;

1.5.5 **"Information Officer"** means Spark's Head as defined in section 1 of POPIA and referred to in paragraph 2.3;

1.5.6 **“PAIA”** means the Promotion of Access to Information Act, No 2 of 2000, as amended and replaced from time to time;

1.5.7 **“Personal Information**” has the meaning ascribed thereto in section 1 of POPIA;

1.5.8 **"Personal Requester**" means a Requester requesting access to a record containing personal information relating to the Requester;

1.5.9 “**POPIA**” means the Protection of Personal Information Act, No 4 of 2013;

1.5.10 “**Processing**” has the meaning ascribed thereto in section 1 of POPIA;

1.5.11 "**Private Body**" means Spark;

1.5.12 “**Record**” has the meaning ascribed thereto in section 1 of PAIA and includes Personal Information;

1.5.13 **“Responsible Party”** has the meaning ascribed thereto in section 1 of POPIA;

1.5.14 "**Requester**" means a person making a request in terms of PAIA for access to information held by Spark, or any person acting on behalf of such a person;

1.5.15 **"Request Fee**" means a fixed fee payable by a Requester (other than a Personal Requester) in terms of section 54(1) of PAIA, set out in "**A**";

1.5.16 "**SAHRC**" means the South African Human Rights Commission;

1.5.17 **"Spark"** means Spark ATM Systems (Pty) Ltd (registration number: 2005/030567/07), a private company duly registered and incorporated in accordance with the company laws of the Republic of South Africa and having its principal place of business situated at Spark House, 31 Transvaal Street, Paarden Eiland, Cape Town, 7405.

1.6 This manual supercedes and replaces all prior manuals prepared by Spark in terms of section 51 of PAIA.

2. INTRODUCTION AND SPARK'S CONTACT DETAILS

2.1 Spark is South Africa’s leading independent ATM deployer whom imports, distributes, sells and leases automated teller machines (“ATMs”). Spark was acquired by Cardtronics (NASDAQ: CATM) (“Cardtronics”) in January 2017.

2.2 Directors

Mr Marc Christopher Terry
Mr David Edward Bolton
Mr William Peter John Davies
Mr Russel David Berman

2.3	Head of Spark / Information Officer	Mr Russel David Berman
2.4	Spark's postal address:	PO Box 101 Paarden Eiland Cape Town 7420 South Africa
2.5	Spark's physical address:	Spark House 31 Transvaal Street Paarden Eiland Cape Town 7405 South Africa
2.6	Deputy Information Officer:	Mr Evan Glover
	Email address:	Office.Privacy@ncr.com

3. GUIDE PUBLISHED BY SOUTH AFRICAN HUMAN RIGHTS COMMISSION

3.1 The SAHRC has compiled a guide in terms of section 10 of PAIA, which guide contains such information that may be relevant to a Requester who wishes to exercise any right contemplated in PAIA.

3.2 Requests in terms of PAIA shall be made in accordance with prescribed procedures set out in paragraph 7 below.

3.3 The guide is available for inspection *inter alia* at the offices of the SAHRC, Braampark Forum 3, 33 Hoofd Street, Braamfontein, and on its website at www.sahrc.org.za

4. RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION

4.1 Where required to do so, Spark keeps records of information to the extent required by the legislation, including but not limited to, the legislation attached to this manual marked Annexure "**C**".

5. ACCESS TO RECORDS HELD BY SPARK AND GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF PAIA

5.1 To assist a Requester to determine the records or information to which it requires access, Spark has classified and grouped its records and information attached to this manual marked Annexure "**D**".

5.2 Please note that a Requester is not automatically allowed to access these records. Access may be refused in accordance with the provisions of sections 63 to 69 of PAIA.

5.3 The following are the grounds on which Spark may, subject to the exceptions contained in Chapter 4 of PAIA, refuse a Request for Access in accordance with Chapter 4 of PAIA:

5.3.1 mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of Personal Information would be unreasonable;

5.3.2 mandatory protection of the commercial information of a third party, if the Records contain:

5.3.2.1 trade secrets of that third party;

5.3.2.2 financial, commercial, scientific or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/or

5.3.2.3 information disclosed in confidence by a third party to Spark, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition;

5.3.3 mandatory protection of confidential information of third parties if it is protected in terms of any agreement;

5.3.4 mandatory protection of the safety of individuals and the protection of property;

5.3.5 mandatory protection of Records that would be regarded as privileged in legal proceedings;

5.3.6 protection of the commercial information of Spark, which may include:

5.3.6.1 trade secrets;

5.3.6.2 financial/commercial, scientific or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of Spark;

5.3.6.3 information which, if disclosed, could put Spark at a disadvantage in contractual or other negotiations or prejudice Spark in commercial competition; and/or

5.3.6.4 computer programs which are owned by Spark, and which are protected by copyright and intellectual property laws;

5.3.7 research information of Spark or a third party, if such disclosure would place the research or the researcher at a serious disadvantage; and

5.3.8 Requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

6. AUTOMATIC ACCESS TO RECORDS HELD BY SPARK

6.1 As at the date of this manual, no notices have been published in terms of section 52(2) of PAIA entitling a Requester to access any information or records of Spark without following the requirements of PAIA.

6.2 General information relating to Spark may be accessed via the internet at www.sparkatm.co.za, which information is available to all persons who have access to the internet.

7. PROCEDURE FOR REQUESTING ACCESS TO SPARK'S RECORDS

7.1 Please note that this paragraph is a guideline only. When requesting access to the Spark's records, the Requester must comply with all the procedural requirements contained in PAIA relating to the request for such access.

7.2 The Requester must complete Form "C" attached to this manual marked Annexure "**B**" and submit the completed Form "C" to the contact person specified in paragraph 2.3 and 2.6, at the address reflected in paragraph 2 of this manual.

7.3 The Requester must provide sufficient detail on Form "C" to enable the contact person to identify:

7.3.1 the Requester;

7.3.2 the record/s requested;

7.3.3 the form of access required by the Requester, if the request is granted; and

7.3.4 the Requester's postal address and/or fax number.

7.4 The Requester must clearly indicate:

7.4.1 that the Requester requires the requested information in order to exercise or protect a right;

7.4.2 the nature of the right which the Requester is seeking to exercise or protect; and

7.4.3 why the requested record is necessary to exercise or protect such right.

7.5 If the request for access is being made on behalf of another person, the Requester must submit proof of the capacity in which the Requester is making the request, to the reasonable satisfaction of the Head/Information Officer and/or Deputy Information Officer.

7.6 Before processing a request, the Head/Information Officer and/or Deputy Information Officer must notify the Requester (excluding a Personal Requester) of the Request Fee payable in order to process the request as set out in Annexure "**A**". A request will not be processed until the Request Fee is paid.

7.7 If Spark has searched for the requested records and in the opinion of the Head/Information Officer and/or Deputy Information Officer, the preparation of the records for disclosure, including arrangements to make the records available to the Requester in the requested form, requires more than the hours prescribed in PAIA for this purpose, the Head/Information Officer and/or Deputy Information Officer shall notify the Requester (other than a Personal Requester) to pay as a deposit an amount not exceeding one third of the Access Fee which would be payable if the request is granted.

7.8 The period set out in paragraph 7.7 may be extended for a further period of not more than 30 (thirty) days, in writing by the Head/Information Officer and/or Deputy Information Officer to the Requester, if the request for access is for a large number of Records or the request for access requires a search for Records held at another office of Spark and the records cannot reasonably be obtained within the original 30 (thirty) day period.

7.9 When the Head/Information Officer and/or Deputy Information Officer has made a decision, the Head/Information Officer and/or Deputy Information Officer shall advise the Requester in writing whether or not the request for access to the records of Spark has been granted. Such decision shall be made within 30 (thirty) days of receipt of the request for access and the Head/Information Officer and/or Deputy Information Officer must give notice to the Requester with reasons (if required) to that effect.

7.10 If the request for access is granted, the Requester must pay an Access Fee in respect of the search, reproduction and preparation of the records requested.

7.11 The Head/Information Officer and/or Deputy Information Officer may withhold access to the requested records of Spark until the applicable fees have been paid.

7.12 If a deposit has been paid in respect of a request for access to Spark's records which has been refused, the deposit shall be refunded to the Requester.

8. INFORMATION OR RECORDS NOT FOUND

8.1 If Spark cannot find the records that the Requester is looking for despite reasonable and diligent search and it believes that the records are in its possession but unattainable, the Requester will receive a notice in this regard from the Head/Information Officer and/or Deputy Information Officer in the form of an affidavit setting out the measures taken to locate the document and accordingly the inability to locate the document.

9. REMEDIES AVAILABLE TO THE REQUESTER UPON REFUSAL OF A REQUEST FOR ACCESS IN TERMS OF PAIA

9.1 Spark does not have internal appeal procedures. As such, the decision made by the Head/Information Officer and/or Deputy Information Officer is final, and Requesters will have to exercise such external remedies at their disposal if the Request for Access is refused.

9.2 In accordance with sections 56(3) (c) and 78 of PAIA, a Requester may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

10. AVAILABILITY OF THIS MANUAL

10.1 This manual is available:

10.1.1 on Spark's website at www.sparkatm.co.za; or

10.1.2 at the offices of Spark during office hours on request and at no charge; or

10.1.3 from the offices of the SAHRC on request and at no charge.

11. PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY SPARK

11.1 Chapter 3 of POPIA provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party. These conditions may not be derogated from unless specific exclusions apply as outlined in POPIA.

11.2 Spark needs Personal Information relating to both individual and juristic persons in order to carry out its business and organisational functions. The manner in which this information is Processed and the purpose for which it is Processed is determined by Spark. Spark is accordingly a Responsible Party for the purposes of POPIA and will ensure that the Personal Information of a Data Subject:

11.2.1 is processed lawfully, fairly and transparently. This includes the provision of appropriate information to Data Subjects when their data is collected by Spark, in the form of privacy or data collection notices. Spark must also have a legal basis (for example, consent) to process Personal Information;

11.2.2 is processed only for the purposes for which it was collected;

11.2.3 will not be processed for a secondary purpose unless that processing is compatible with the original purpose;

11.2.4 is adequate, relevant and not excessive for the purposes for which it was collected;

11.2.5 is accurate and kept up to date;

11.2.6 will not be kept for longer than necessary;

11.2.7 is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that Personal Information, in both physical and electronic form, are subject to an appropriate level of security when stored, used and communicated by Spark, in order to protect against access and acquisition by unauthorised persons and accidental loss, destruction or damage;

11.2.8 is processed in accordance with the rights of Data Subjects, where applicable. Data Subjects have the right to:

11.2.8.1 be notified that their Personal Information is being collected by Spark. The Data Subject also has the right to be notified in the event of a data breach;

11.2.8.2 know whether Spark holds Personal Information about them, and to access that information. Any request for information must be handled in accordance with the provisions of this manual;

11.2.8.3 request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained Personal Information;

11.2.8.4 object to Spark's use of their Personal Information and request the deletion of such Personal Information (deletion would be subject to Spark's record keeping requirements);

11.2.8.5 object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications; and

11.2.8.6 complain to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

11.3 Purpose of the Processing of Personal Information by Spark

11.3.1 As outlined above, Personal Information may only be Processed for a specific purpose. The purposes for which Spark Processes or will Process Personal Information is set out in **Part 1 of Annexure "E".**

11.4 Categories of Data Subjects and Personal Information/special Personal Information relating thereto

11.4.1 As per section 1 of POPIA, a Data Subject may either be a natural or a juristic person. **Part 2 of Annexure "E"** sets out the various categories of Data Subjects that Spark Processes Personal Information on and the types of Personal Information relating thereto.

11.5 Recipients of Personal Information

11.5.1 Part **3 of Annexure "E"** outlines the recipients to whom Spark may provide a Data Subjects Personal Information to and when Personal Information has been received from third parties to Spark.

11.6 Cross-border flows of Personal Information

11.6.1 Section 72 of POPIA provides that Personal Information may only be transferred out of the Republic of South Africa if the:

11.6.1.1 recipient country can offer such data an “adequate level” of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in POPIA; or

11.6.1.2 Data Subject consents to the transfer of their Personal Information; or

11.6.1.3 transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or

11.6.1.4 transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or

11.6.2 the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

Part 4 of Annexure “E” sets out the planned cross-border transfers of Personal Information and the condition from above that applies thereto.

11.7 Description of information security measures to be implemented by Spark

11.7.1 Part **5 of Annexure “E”** sets out the types of security measures to implemented by Spark in order to ensure that Personal Information is respected and protected. A preliminary assessment of the suitability of the information security measures implemented or to be implemented by Spark may be conducted in order to ensure that the Personal Information that is processed by Spark is safeguarded and Processed in accordance with the Conditions for Lawful Processing.

11.8 Objection to the Processing of Personal Information by a Data Subject

11.8.1 Section 11 (3) of POPIA and regulation 2 of the POPIA Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed form attached to this manual as **Annexure “F”** subject to exceptions contained in POPIA.

11.9 Request for correction or deletion of Personal Information

11.9.1 Section 24 of POPIA and regulation 3 of the POPIA Regulations provides that a Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form attached as **Annexure “G”** to this Manual.

Signed at _____on this ____ day of _____2022

by Russel Berman in his capacity as Managing Director of Spark.

_____

Russel Berman

ANNEXURE "A"

FEES

REPRODUCTION FEES

In terms of section 52 of PAIA, the head of a private body may, on a voluntary and periodic basis, submit to the Minister of Justice a description of the categories of records of the private body concerned that are automatically available without a person having to request access thereto in terms of PAIA.

If the private body has voluntarily provided the Minister of Justice with a list of categories of records that will automatically be made available to any person requesting access thereto, the only charge that may be levied for obtaining such records, will be a fee for reproduction of the record in question. The applicable fees for reproduction referred to above are set out below.

	R
• For every photocopy of an A4-size page or part thereof	1,10
• For every printed copy of A4-size page or part thereof held on a computer or in electronic or machine readable form	0,75
• A transcription of visual images, for A4-size page or part thereof	40,00
• For a copy of visual images	60,00
• A transcription of an audio record, for A4-size page or part thereof	20,00
• For a copy of an audio record	30,00

REQUEST FEES

Where a requester submits a request for access to information held by the group in respect of a person other that the requester himself, a request fee in the amount of R50,00 is payable up-front before the group will further process such request.

ACCESS FEES

An access fee is payable in all instances where a request for access to information is granted, except in those instances where payment of an access fee is specially excluded in terms of PAIA or an exclusion is determined by the Minister in terms of section 54(8). The applicable access fees which are payable are set out below.

	R
• For every photocopy of an A4-size page or part thereof	1,10
• For every printed copy of A4-size page or part thereof held on a computer or in electronic or machine readable form	0,75
• A transcription of visual images, for A4-size page or part thereof	40,00
• A transcription of an audio record, for A4-size page or part thereof	20,00
• For a copy of visual images	60,00
• For a copy of an audio record	30,00
• To search for and prepare a record that must be disclosed (per hour or part of an hour reasonably required for such search and preparation)	30,00
• Where a copy of a record needs to be posted the actual postal fee is payable	

DEPOSITS

If the group receives a request for access to information held in respect of a person other than the requester himself and the Chairperson or Information Officer, upon receipt of such request, is of the opinion that the preparation of the requested record for will take more than six hours, a deposit is payable by the requester.

The amount of the deposit shall not exceed one third of the amount of the applicable access fee.

VAT

Value-added tax shall be added to all fees prescribed in terms of the regulations to PAIA.

ANNEXURE "B"

PRESCRIBED FORM C – ACCESS REQUEST FORM

REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of PAIA

ANNEXURE "C"

LIST OF APPLICABLE LEGISLATION

Basic Conditions of Employment Act 75 of 1997
Broad-Based Black Economic Empowerment Act 53 of 2003
Companies Act 71 of 2008
Compensation for Occupational Injuries and Diseases Act 130 of 1993
Competition Act 89 of 1998
Constitution of South Africa Act 108 of 1996
Consumer Protection Act 68 of 2009
Copyright Act 98 of 1987
Currency & Exchanges Act 9 of 1933
Customs and Excise Act 91 of 1964
Electronic Communications and Transactions Act 2 of 2000
Employment Equity Act 55 of 1998
Income Tax Act 58 of 1962
Labour Relations Act 66 of 1995
Occupational Health and Safety Act 85 of 1993
Pensions Funds Act 24 of 1956
Prescription Act 18 of 1943
Prevention of Organised Crime Act 121 of 1998
Promotion of Access to Information Act 2 of 2000
Protection of Personal Information Act 4 of 2013
South African Reserve Bank Act 90 of 1989
Unemployment Insurance Fund Contributors Act 4 of 2002
Value Added Tax Act 89 of 1991

This list is not exhaustive and whenever it comes to our attention that existing or new legislation allows a Requester access on a basis other than as set out in PAIA, we shall update the list accordingly. If a Requester believes that a right of access to a record exists in terms of other legislation listed above or any other legislation, the Requester is required to indicate what legislative right the request is based on, to allow the Information Officer the opportunity of considering the request in light thereof.

ANNEXURE "D"

1 **Customer / Supplier Records**

1.1 Customer /Supplier correspondence;

1.2 Customer /Supplier contracts;

1.3 Customer /Supplier business information and details;

1.4 Service contracts;

1.5 Supply and purchase agreements;

1.6 Proposal and tender documents;

1.7 Project plans;

1.8 Risk management records;

1.9 Working papers;

1.10 Banking records.

2 **Corporate Governance / Administration**

2.1 Spark administration policies and procedures;

2.2 Board resolutions, minute books, asset register, minutes of meetings

2.3 Statutory documents (certificates of incorporation) and corporate structure

2.4 Statutory returns to relevant authorities

2.5 Legal compliance records / Powers of Attorney;

2.6 Codes of conduct;

3 **Finance and Administration**

3.1 Accounting records;

3.2 Annual financial statements;

3.3 Debtors and creditors information;

3.4 Correspondence, agreements;

3.5 Purchase orders;

3.6 Remittances, invoices and statements;

3.7 Invoices and statements;

3.8 Tax files, VAT, PAYE, Income tax records and returns;

3.9 Insurance polices

3.10 Contact details of internal and external auditors;

4 **Human Resources**

4.1 Employee records;

4.2 Contracts of employment;

4.3 Training records, manuals, materials and reports;

4.4 Employment equity records and reports;

4.5 Recruitment records;

4.6 Disciplinary records;

4.7 Annual leave, sick leave, paternal leave and special leave records

4.8 Payroll and PAYE records and returns;

4.9 Performance management and career records;

4.10 Assessments, policies and procedures;

4.11 UIF returns;

4.12 Retirement benefit;

4.13 Medical Aid records; and

4.14 CCMA, litigation, mediation and arbitration records.

5 **Information Management and Technology**

5.1 Agreements, Information technology systems and User manuals;

5.2 Equipment register, software licenses, permits;

5.3 Information policies; and

5.4 IT Standards, procedures and guidelines.

6 **Learning and Education**

6.1 Training material;

6.2 Training records and statistics;

6.3 Learnership programmes and career development.

6.4 Training agreements; and

7 **Marketing and Communication**

7.1 Proposal documents;

7.2 New business development;

7.3 Brand information management;

7.4 Marketing strategies;

7.5 Communication strategies;

7.6 Agreements;

7.7 Client relationship programmes;

7.8 Marketing newsletters, publications and brochures; and

7.9 Sustainability programmes.

7.10 Internet

8 **Operations**

8.1 Access control records;

8.2 Agreements;

8.3 Archival administration documentation;

8.4 Communication strategies;

8.5 General correspondence;

8.6 Patents and Trade Mark documents;

8.7 Insurance documentation;

8.9 Service level agreements;

8.10 Standard trading terms and conditions of supply of services and goods;

8.11 Travel documentation;

8.12 Procurement agreements and documentation;

8.13 Used order books;

8.14 Vehicle registration documents.

ANNEXURE "E"

PART 1

PROCESSING OF PERSONAL INFORMATION IN ACCORDANCE WITH POPIA

This is a list of all the ways that we will use your personal information and the lawful basis for collecting and processing your data.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To manage our relationship with you or your business, take orders, process and deliver products and services to you including complaint and dispute resolution. Managing how we work with other companies that provide services to us and our customers	Contact and identity data, documentation, financial data, usage and technical data	(a) Performance of a contract with you e.g. making payments, service communications (b) Necessary for our legitimate interests e.g. KYC (c) Legal obligation – record retention
To administer and protect our business and the website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	Identity and contact data, technical and usage data	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
Security and risk management including detection and investigation and reporting of financial crime. Managing risk for us and our customers.	Contact and identity data, documentation, financial data, usage and technical data, CCTV images.	(a) Performance of a contract (b) Necessary for our legitimate interests including crime prevention and detection) (c) Legal obligation
To develop new ways to meet our customers' needs and grow our business, develop new products and services.	Usage and technical data.	(a) Necessary for our legitimate interests

We will only use your Personal Information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact Spark.
If we need to use your Personal Information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

PART 2

Categories of Data Subjects and categories of Personal Information relating thereto

We collect contact details in each case and then supplementary information required for the purposes of fulfilling the relationship Spark has with you which may in the case of an employment relationship include special information categories of data.

We also collect, use and share statistical or demographic data. This may be derived from your Personal Information but is not considered Personal Information in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your Personal Information so that it can directly or indirectly identify you, we treat the combined data as Personal Information which will be treated and used in accordance with POPIA.

Data Type	Description
Contact Details	Natural and Juristic Persons: Your name/company name, physical address, how to contact you i.e. email, phone
Financial	Bank account and branch code details
Contractual	Signed agreements for the services we provide you
KYC supporting documents	Details about you taken from documents such as company registration number, ID number, passport number, driving license or birth certificate, utility bills.
Land Ownership	Property details and names of ownership
Communication	What we find out about you from letters, phone calls and emails we received from you.
Consent	Any permissions or consent you have provided us.
CIPC	Business/organisation information, business/organisation structure
Special Personal Information	Biometric information and race.

PART 3

Recipients of Personal Information

We have to share your Personal Information with the parties set out below for the purposes set out in the table above.

- Internal Third Parties: other companies in the Cardtronics group acting as operators and who provide IT, system administration and other services to Spark and the Cardtronics group and its customers.
- External Third Parties: service providers, acting as operators who provide services to Spark and its customers.
- Professional advisers acting as operators including lawyers, bankers, fraud and other crime prevention agencies, auditors and insurers.
- South African Revenue Services, regulators and other authorities acting as opertors who require reporting of certain activities.
- Agents and advisers who we use to help run your accounts and services, collect what you owe, and explore new ways of doing business.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your Personal Information in the same way as set out above.

We require all third parties to respect the security of your Personal Information and to treat it in accordance with the law. We do not allow our third-party service providers to use your Personal Information for their own purposes and only permit them to process your Personal Information for specified purposes and in accordance with our instructions.

When Spark receives Personal Information from a third party on behalf of a data subject, it requires confirmation that the third party has a lawful justification and/or agreement from the data subject that they are aware of the contents of this PAIA manual, the Spark privacy policy, the applicable legislation and do not have any objection to Spark processing the data subject Personal Information in accordance with the Spark privacy policy.

PART 4

Cross border transfers of Personal Information

When making authorised disclosures or transfers of personal information in terms of section 72 of POPIA, Spark will only transfer Personal Information across South African borders if the relevant transactions or situation requires trans-border processing. Spark will only do so in accordance with South African legislative requirements, or if the Data Subject consents to the transfer of their Personal Information to third parties in foreign countries

Spark will take steps to ensure that operators (suppliers and third parties) in foreign countries are bound by laws, binding corporate rules or binding agreements that provide an adequate level of protection of Personal Information and uphold principles for reasonable and lawful processing of personal information, in terms of POPIA.

Spark will take steps to ensure that operators (suppliers and third parties) that process Personal Information in jurisdictions outside of South Africa, apply adequate safeguards as outlined in paragraph Part 5 below.

PART 5

Description of information security measures

Spark undertakes to institute and maintain the data protection measures to accomplish the following objectives outlined below. Spark has put in place appropriate security measures to prevent your Personal Information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Spark may use alternative measures and adapt to technological security development, as needed, provided that the objectives are achieved. In addition, Spark shall limit access to your Personal Information to those employees, agents, contractors and other third parties who have a business need to know. Such parties will only process your Personal Information on our instructions and they are subject to a duty of confidentiality. Spark has put in place procedures to deal with any suspected Personal Information breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

1. **Access Control of Persons**

1.1 Spark shall implement suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment where the data are processed.

1.2 Spark follows a formal process to grant or revoke access to Spark resources. System access is based on the concepts of least-privilege, so that authorised access is commensurate with defined responsibilities.

1.3 Spark has established documented procedures for secure creation and deletion of user accounts, including processes to disable and/or delete accounts for terminated personnel.

1.4 Spark security policy establishes password requirements that include password change, reuse and complexity.

2. **Organisation Control**

2.1 Spark maintains a dedicated Information Security group, led by its Chief Information Security Officer. The Information Security team includes specialists in threat and vulnerability management, incident response, application security and Information Security risk management.

2.2 Spark Information Security group have defined a set of information security policies and standards to support information security across the global business

3. **Human Resources Security**

3.1 Spark personnel receiving access to client information undergo pre-employment background checks.

3.2 All Spark employees are required to agree to maintain the confidentiality of client information and to complete information security and privacy awareness training.

4. **Physical and Environmental Security.**

4.1 Spark data centres are surrounded by perimeter fencing, and require biometric and key card access through multiple gates to enter their facilities. Access to Spark data centres are restricted to authorised personnel only.

4.2 Security systems and supporting controls are implemented in all Spark sites to provide access control, video monitoring and auditing services.

4.3 Offices are not accessible to general public and Spark operates a “clean desk” policy to minimise risk to unauthorised access to data and operates a confidential and secure document shredding facility.

5. **Operations Management.**

5.1 Spark IT organisation has established and maintains standard operating procedures which include a repository of procedures, formal review and approval processes, and revision management, as well as a change control process, which includes risk assessment, test and back out procedures, communication planning, management review, and approval components.

5.2 Spark maintain separate development and production environments. Lab environments are separated from production environments by firewalls. Spark has established procedures requiring the use of the change management process to transfer changes from development to production.

5.3 Spark uses enterprise class security solutions to provide a secure computing environment. These solutions are centrally managed and configured to retrieve updates automatically. Spark laptops and desktops run a security suite which includes virus protection anti-spyware, firewalls, host intrusion detection, application whitelisting, endpoint rights management, privileged user management, whole disk encryption and advanced threat detection. Spark server systems run server class versions of the antivirus and application whitelisting solutions used for laptops.

5.4 Spark systems are configured to use a network time server designed to ensure log synchronization for event correlation. Spark maintains system audit logs for servers and network devices that log the occurrence of system faults and security events and facilitate examination of abnormal

activities. Security logs are collected to a central security information and event management (SIEM) system to prevent modification or removal of administration and user activities.

5.5 Spark have established processes and procedures for performing periodic vulnerability scans of its IT systems, which specify the use of multiple vulnerability scanning software packages, the creation of vulnerability assessment reports, and the presentation of vulnerability scanning results to the IT operations organization and IT leadership. Vulnerability scanning of networked devices is performed on a monthly basis.

5.6 Spark has patch management processes and tools to assess and deploy operating system and application-specific patches and updates. Spark continually reviews and risk assesses patches and updates as they are released to determine their criticality. Patches released on a regularly scheduled basis are applied following the release; off-cycle or other patches determined to be critical are applied as needed to ensure protection from vulnerabilities.

6. **Communications Security.**

6.1 Only IT-approved and managed wireless networks are permitted on the Spark network, and technologies are in place to identify and disable ports with rogue wireless networks attached. Wireless access security controls are centrally managed and use WPA2 for encryption and authentication.

6.2 All internet ingress points feature firewall segregation. Intrusion detection system appliances are located at strategic points in the network. The intrusion detection system feeds a central SIEM system that is monitored by the Information security team. Firewall logging is enabled to track communications (failed and successful access attempts) between the Internet and the internal Spark network. Console access to the firewalls is restricted to a small number of authorised individuals

6.3 Spark requires encryption in transit of client Personal Information transmitted over public or wireless networks. Spark uses virtual private network (VPN) to enable secure, Internet-based remote access to the Spark internal network by Spark personnel and contractor endpoints.

7. **Supplier Relationships.**

7.1 Spark has implemented security controls designed to ensure that external parties who provide IT and other back office services to Spark do so in a manner consistent with Sparks' standards for the security of information systems. Spark's vendor management program is designed to ensure that external parties meet Spark's standards through risk categorisation, due diligence, contractual requirements, and ongoing monitoring and assessments.

7.2 Access to Spark systems is controlled using a least privilege principle (e.g., providers are only permitted a level of access to systems consistent with the business need for access). Access is controlled at the physical, network, platform and application levels.

7.3 Suppliers that process data on behalf of Spark will be issued with data processing addendums to their existing contracts with Spark to ensure that any processing they undertake is compliant with POPIA and that any international transfers of data, including those to any sub-operators, are covered by adequate and sufficient data protection mechanisms.

8. Business Continuity.

8.1 Spark maintains a Business Continuity Program that evaluates and manages potential threats and responds to actual events to minimise disruption to Spark services and operations, and is designed so that, should a disaster occur, Spark can continue to deliver on client obligations.

ANNEXURE "F"

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

Note:

1 Affidavits or other documentary evidence as applicable in support of the objection may be attached.

2 If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3 Complete as is applicable.

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ registered name of data subject:	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)**

SIGNED AT ..... THIS ..... DAY OF .....20……...

.....

Signature of data subject/designated person

ANNEXURE "G"

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

Regulation 3

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

Mark the appropriate box with an "x".

REQUEST FOR:

☐ **Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.**

☐ **Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.**

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ registered name of data subject:	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	

C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)

D	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. (Please provide detailed reasons for the request)

Date of Compilation: 7/11/2020