



Group Protection of Personal Information Act Policy

TABLE OF CONTENTS

1. PURPOSE, SCOPE AND APPLICATION.....	3
2. TERMINOLOGY	4
3. RESPONSIBILITIES.....	7
4. POLICY STATEMENT	8
5. PROCEDURES.....	9
6. ADDITIONAL GUIDELINES	12
7. REVIEW OF POLICY.....	12

1. PURPOSE, SCOPE AND APPLICATION

The purpose of this document is to outline the policy (“Policy”) on the Protection of Personal Information Act (hereinafter referred to as “PoPIA”) for DR Gaming Technology Group (“DRGT”). The DRGT is committed to the highest legal, ethical, and moral standards. This Policy is applicable to all the subsidiaries of DRGT Africa and Infinity Gaming Africa.

The Protection of Personal Information Act is South Africa’s data protection law enacted in 2013. It will come into effect in its entirety, by presidential proclamation. It regulates how anyone who processes personal information must handle, keep, and secure this personal information. PoPIA makes provision for what is called ‘special person information’ such as religious beliefs, trade union membership persuasion etc. There is a general prohibition on the processing of special personal information unless explicit prior consent is obtained.

PoPIA impacts on any personal information that is being gathered by companies. It clearly outlines:

- The manner in which information should be stored;
- What care should be taken in dealing with that information;
- When that information has to be purged; and
- Allows for no deviation from these rules.

The purpose of PoPIA is to protect personal information, to strike a balance between the right to privacy and the need for the free flow of, and access to information, and to regulate how personal information is processed.

The Policy establishes a general standard on the appropriate protection of personal information within DRGT. It provides the principles regarding the right of individuals to privacy and to reasonable safeguards of their personal information.

It gives effect to the right to privacy in terms of the South African common law, section 14 of the Constitution and the purpose and application of the Protection of Personal Information Act, No 4 of 2013. It gives effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible third-party and it regulates the manner in which personal information may be processed, by establishing conditions, in harmony with international standards that prescribe the minimum threshold requirements for the lawful processing of personal information.

The Policy further provides persons with rights, responsibilities, and remedies to protect their personal information from processing that is not in accordance with the Act and communicate DRGT's commitment to data protection.

Furthermore, the Policy ensure that DRGT complies with the law in respect of the data DRGT holds on behalf of clients and employees and protects DRGT from the consequences of a breach of its responsibilities.

2. TERMINOLOGY

- 2.1 Unless otherwise determined by the context, the words and expressions used in this Policy shall bear the meaning assigned to them below -
- 2.1.1 "child" means a natural living person under the age of 18;
 - 2.1.2 "consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
 - 2.1.3 "data subject" means a person to whom personal information relates;
 - 2.1.4 "de-identify" means to delete any personal information that identifies a data subject, or which can be used by a reasonably foreseeable method to

identify, or when linked to other information, that identifies the data subject and the term "de-identified" shall have a corresponding meaning;

- 2.1.5 "direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: (i) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (ii) requesting the data subject to make a donation of any kind for any reason;
- 2.1.6 "information officer" means the Head of DRGT, whose responsibility is to ensure the organisation's compliance with PoPIA;
- 2.1.7 "information regulator" means the information regulator established in terms of section 39 of PoPIA;
- 2.1.8 "legitimate basis" means any of the following legitimate bases recognised by PoPIA for the processing of personal information -
- 2.1.8.1 the data subject, or a competent person where the data subject is a child, consents to the processing; or
 - 2.1.8.2 the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
 - 2.1.8.3 the processing complies with an obligation imposed by law on the responsible party; or
 - 2.1.8.4 the processing protects a legitimate interest of the data subject;
- or
- 2.1.8.5 the processing is necessary for pursuing the legitimate interests of DRGT or of a third party to whom the information is supplied.
- 2.1.9 "operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party;
- 2.1.10 "personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to -
- 2.1.10.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual

- orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- 2.1.10.2 information relating to the education or the medical, financial, criminal or employment history of the person;
- 2.1.10.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- 2.1.10.4 the biometric information of the person;
- 2.1.10.5 the personal opinions, views or preferences of the person;
- 2.1.10.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- 2.1.10.7 the views or opinions of another individual about the person; and
- 2.1.10.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
- 2.1.11 "processing / process" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including
- 2.1.11.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- 2.1.11.2 dissemination by means of transmission, distribution or making available in any other form; or
- 2.1.11.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;
- 2.1.12 "re-identify" means, in relation to personal information of a data subject, to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject;

- 2.1.13 "responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing of personal information; and
- 2.1.14 "special personal information" means personal information relating to: (i) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (ii) the criminal behaviour of a data subject to the extent that such intimation relates to: (a) the alleged commission by a data subject of any offence; or (b) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. RESPONSIBILITIES

Board of Directors

The board of directors (the "Board") is ultimately responsible for ensuring that all financial, reputational, and other risks are appropriately managed ("Risk Management") and for ensuring that the requisite systems, practices, and culture are in place for Risk Management. The Board is also ultimately responsible for ensuring that DRGT complies with all applicable laws and regulations ("Compliance"). The Board may delegate Risk Management and Compliance to individuals, committees, consultants, but the ultimate responsibility still vests with the Board.

Information Officer

The Group Financial Manager: Africa has been duly appointed as the Information Officer by the Chief Executive Officer, to act as the person to whom requests for access to information must be made in terms of the Act.

The Information Officer is responsible for:

- assessing DRGT's internal business management and control processes and the extent to which Remedial Action has been implemented; and
- for reporting thereon to the Board.

Management

Management is responsible for publishing, enforcing, regularly reviewing and, where necessary, updating the Policy.

Employees

Employees are expected to comply with DRGT's obligations under DRGT's protection of information and data security framework (including all internal rules and policies adopted under such framework) as well as with any additional controls, processes and procedures that may be implemented by the Information Officer and management. All employees have a responsibility for the management and lawful processing of personal information.

4. POLICY STATEMENT

DRGT respects and recognises the importance of protecting the privacy and data of its employees, clients, members, and all external clients. The right of privacy is enshrined in the South African Constitution which expressly states that everyone has the right to privacy. The legislation contained in PoPIA is aimed at facilitating the protection of this important right.

DRGT has identified a need to create consistent standards and rules within the workspace. For this reason, DRGT will implement policies addressing the protection of its people's personal information and data.

5. PROCEDURES

5.1 Types of Records

- Attendance and training registers
- Correspondence
- Founding documents
- Licences (categories)
- Minutes of meetings
- Statutory returns
- Conditions of service
- Employment contracts
- Information relating to health and safety regulations
- Pension and provident fund records
- Performance appraisals and remuneration records
- Personnel guidelines, policies, and procedures
- Skills requirements
- Staff recruitment policies
- Training Records
- Marketing and future strategies
- Annual financial statements

5.2 Types of Information to be protected

Section 26 of PoPIA creates a special category of personal information called "special personal information". This relates to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information. Also included in this category is information

relating to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed and the outcome of such proceedings.

Failure to obtain consent makes processing this special personal information strictly prohibited, unless,

- it is necessary by law;
- or is done for historical, statistical or research purposes;
- or the information has been deliberately made public by the subject.

Therefore, the following information needs to be strictly protected at all times by DRGT -

- Identity and / or passport number
- Date of birth and age
- Phone number(s) and email address(es)
- Physical address
- Gender, race, and ethnic origin
- Marital / relationship status and family relations
- Criminal record
- Private correspondence
- Employment history and financial information
- Biometric information

5.3 Disclosure of Personal Information

5.3.1 DRGT is not in the business of selling personal information and therefore we will not disclose any personal information and data to anyone except as provided in this Policy.

5.3.2 We may for administration purposes disclose or transfer personal information to our clients.

5.3.3 It may be necessary for us to disclose or transfer personal information to suppliers, affiliates, partners, or agents in order to serve our clients and to provide our members with quality service.

5.3.4 We will need to disclose personal information to our employees who require it to do their jobs. We make sure they are aware of and take their confidentiality obligations seriously. They are contractually bound to keep all confidential information confidential.

5.3.5 There may be situations where the law requires us to disclose personal information and data. In all other situations, we will not disclose personal information without notifying the data subject or the relevant parties and enabling owners of the personal information into object and consent.

5.4 Security of Personal Information

5.4.1 DRGT undertakes all reasonable and appropriate measures to secure personal information. We encrypt our laptops and our phones. However, it is important to highlight that to ensure absolute security of it we shall back-up all personal information and data on a regular basis.

5.4.2 We are also legally obliged to provide adequate protection for the Personal Information and to stop unauthorised access and use of personal information.

5.4.3 Our security policies and procedures cover:

- Physical security
- Access to personal information
- Secure communications
- Monitoring access and usage of personal information
- Computer and network security
- Security in contracting out activities and functions
- Governance and regulatory issues

5.4.4 When we contract with third parties, we impose appropriate security, privacy, and confidentiality obligations on them to ensure that personal information we remain responsible for is kept secure.

5.4.5 The discipline of Information Security aims to protect the:

- Confidentiality of information, by ensuring that information is accessible only to those authorised to have access to the information;
- Integrity of information, by safeguarding the accuracy and completeness of information; and
- Availability of information, by ensuring that authorised users have access to information and information systems required to process information, as and when needed.

6. ADDITIONAL GUIDELINES

This Policy is in addition to, and must be read with PoPI Guidelines – Appendix A.

7. REVIEW OF POLICY

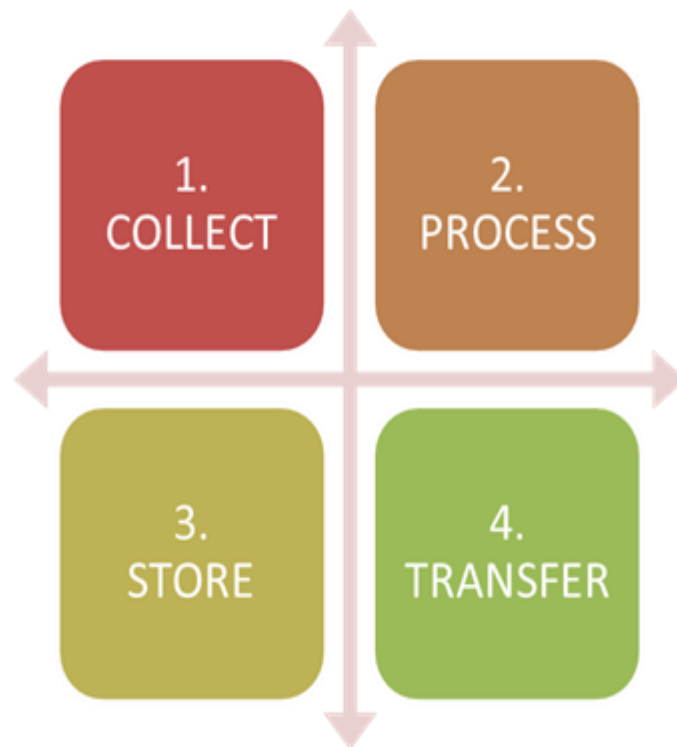
This policy will be reviewed annually by the Board. Any changes to the Policy will be communicated to all employees.

“APPENDIX A”

POPI GUIDELINES

1. The PoPI Framework

The protection of personal information framework occurs at both an organisational level (top-down) and business unit level (bottom-up). It comprises the following steps:



STEP 1: COLLECT

- The first relevant area concerns the collection of personal information.
- Data collection is the process of gathering and measuring information.
- Under PoPIA, such information may only be collected for the specific purpose of providing services to a particular subject.
- A specific new obligation created by PoPIA is that once personal information has been collected from another source, DRGT will take reasonable steps to inform the data subject of this, together with the source of the information and the purpose for which it has been collected.
- This processing requires one to answer relevant questions and evaluate outcomes.
- The process of collecting data information includes:
 - Identifying issues and/or opportunities for collecting data;

- Defining the purpose for collection the data; and
- Analysing and interpreting the data.

STEP 2: PROCESS

Personal information can only be processed:

- With the consent of the “data subject”;
- If it is necessary for the conclusion or performance of a contract to which the “data subject” is a party;
- It is required by law;
- It protects a legitimate interest of the “data subject”;
- It is necessary to pursue your legitimate interests or the interest of a third party to whom the information is supplied; and
- Any operation, or activity, or set of operations (whether or not by automatic means).

Processing information includes:

Collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation, or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, erasure, or destruction.

STEP 3: STORE

- This element covers the processing and storing of information, the duration of storage, and the need to inform data subjects that their information is being stored.

- Whenever DRGT establishes a business relationship or concludes a transaction with a client, whether the transaction is a single transaction or concluded in the course of a business relationship which DRGT has with the client, DRGT must keep record of this information.
- DRGT must keep records of the business relationship, for at least five years from the date on which the business relationship is terminated.
- When concluding a transaction, records must be kept for at least five years from the date on which that transaction is concluded.

STEP 4: TRANSFER

- PoPIA makes provision for transfers and applies to the distribution of personal information to third parties who process (collect, store, use or destroy) such information on behalf of DRGT.
- Data transfers are a daily business requirement when transferring personal information.
- Such transfers should take place only where absolutely necessary and employing the most secure channel available.
- To support this, all DRGT employees must adhere to the following: -
 - Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted.
 - Strong passwords must be used to protect the data during transfer. Such passwords must not be sent with the data it is intended to protect. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person.
 - Standard email should never be used to transmit any personal data. Where file encryption or the use of a secure email facility which will encrypt the data (including any attachments) is sent, staff must still ensure that the mail is sent only to the intended recipient.

2. RECORDING INFORMATION

Regardless of when the record came into existence.

A “record” means:

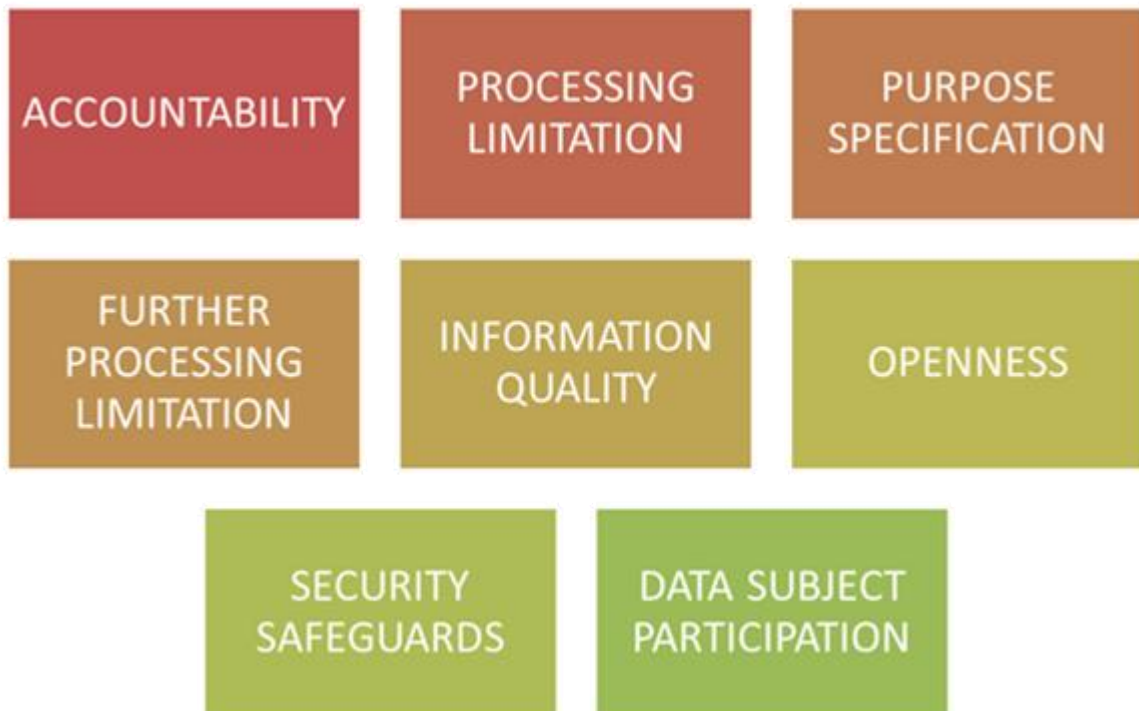
- Any recorded information;
- Regardless of form or medium;
- In the possession or under the control of the private body; and
- Whether or not it was created by the private body.

A record in the possession or under the control of an independent contractor engaged by a private body is regarded as being a record of that private body.

3. TRANS-BORDER FLOWS OF PERSONAL INFORMATION

- PoPIA focusses on the location of processing rather than the location of the data subject.
- Section 72 of PoPIA deals with transfers of personal information outside South Africa or trans-border information flows. A responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless certain protections are in place. For example, if:
 - the foreign country has a law that provides adequate protection;
 - there are binding corporate rules that provide adequate protection;
 - there is an agreement between the sender and the receiver that provides adequate protection;
 - the data subject consents to their personal information being so transferred; or
 - the transfer is necessary for the responsible party to perform in terms of a contract.
 - In light of the above, DRGT must ensure that one or more of the appropriate aforementioned actions have been taken and the applicable measures have been put in place to ensure compliance with PoPIA in the event that it is required to participate in a cross-border transfer of personal information for a beneficiary.

8 (Eight) Conditions for Lawful Processing of Personal Information



1. ACCOUNTABILITY

1.1 DRGT will ensure that all the principles contained in PoPIA and all the measures that give effect to these principles are complied with when:

- Deciding the purpose of processing personal information;
- Deciding how the processing will be done; and
- While the information is being processed.

1.2 DRGT will appoint personnel and task them with the responsibility of compliance.

1.3 This individual will be held liable for non-compliance in certain situations regarding breaches of personal information of data subjects.

2. PROCESSING LIMITATION

- 2.1 The processing of information must be lawful and in a reasonable manner that does not infringe the privacy of the data subject.
- 2.2 Information may only be processed if it is adequate, relevant, and not excessive.
- 2.3 Must have been consented to and collected directly from the subject (subject to provisions).
- 2.4 The processing of information must be justified on the basis of one or more of a number of particular reasons, including the fact that the processing:
 - Is necessary for performing a contract;
 - Complies with a legal obligation;
 - Protects a legitimate interest of the data subject;
 - Is necessary for the performance of a public law duty of a public body is necessary to pursue the 'legitimate interests' of those to whom the information is supplied; and
 - If a data subject has objected to the processing of personal information; DRGT may no longer process the personal information and consent may be withdrawn at any time.
- 2.5 Personal information must be collected directly from the data subject except in certain circumstances, for instance where the information is already available in a public record or where there is consent to collect the information from another source.

3. PURPOSE SPECIFICATION

- 3.1 DRGT will take steps to ensure that the data subject knows the purpose for which the data is being collected.
- 3.2 That the information is collected for a specific and explicitly defined and lawful purpose – related to the activity or function of DRGT.
- 3.3 Records must not be detained for longer than necessary.

4. FURTHER PROCESSING LIMITATION

- 4.1 Personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- 4.2 DRGT will ensure that secondary processing is aligned with the original intent.
- 4.3 It will be in accordance with the purpose for which it was collected.
- 4.4 DRGT will put in place an assessment of further processing.
- 4.5 DRGT must take account of the relationship between purpose of intended further processing and the initial purpose of collection.
- 4.6 In the absence of specific consent for further use DRGT will only use the personal information if it is compatible with or in accordance with the purpose for which it was collected.
- 4.7 Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in the first place.
- 4.8 DRGT will take account of:
 - The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
 - The nature of the information concerned;
 - The consequences of the intended further processing for the data subject;
 - The manner in which the information has been collected; and
 - Any contractual rights and obligations between the parties.

5. INFORMATION QUALITY

- 5.1 DRGT has the responsibility to take reasonably practicable steps to ensure information is complete, accurate and not misleading.
- 5.2 It must be updated where necessary and consider the purpose for which collected.
- 5.3 It will ensure that the information is reliable all the time.
- 5.4 It will have processes in places to ensure that all clients, data subjects and employees are able to update their personal information.

6. OPENNESS

- 6.1 There are a number of requirements which DRGT must meet when personal information is collected from a data subject and there are also reasons for non-compliance with this condition.
- 6.2 This includes that DRGT must take reasonably practicable steps to ensure that the data subject is aware of the fact that the information is being collected and where the information is not collected from the data subject, the source from which it is collected.
- 6.3 DRGT will maintain the documentation of all processing operations under its responsibility.
- 6.4 DRGT take reasonably practicable steps to ensure that the data subject is aware of:
 - The information being collected or the source from which it is collected;
 - The name and address of the responsible party;
 - The purpose for which the information is being collected;
 - Whether or not the supply of the information is voluntary or mandatory; and
 - The consequences of failure to provide the information.

7. SECURITY SAFEGUARDS

- 7.1 DRGT has a duty to secure the integrity and confidentiality of personal information in its possession or under its control.
- 7.2 Where there are reasonable grounds to believe personal information has been accessed by an unauthorized person, DRGT will:
- Notify the Regulator;
 - Notify the data subject; and
 - Take reasonable technical and organisational measures to prevent loss of, damage, unlawful access, or unauthorised destruction.
- 7.3 This includes risk management and steps to identify threats.
- 7.4 The regulator and subject must be informed if there has been or a reasonable expectation of a breach of security.

8. DATA SUBJECT PARTICIPATION

- 8.1 A data subject, with adequate proof of identity has the right to request DRGT to confirm, free of charge, whether they hold personal information of the subject.
- 8.2 Data subject may request the correction or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.
- 8.3 Enquire – free of charge - whether their personal information being processed.
- 8.4 Request description of their personal information.
- 8.5 Request information on recipients of their personal information.
- 8.6 Challenge the accuracy of personal information.

-
- 8.7 Request correction of information (if inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully).