

Policy Statement: Protection of Personal Information Act (POPIA)

in respect of the duties and responsibilities of JVR and
its clients in terms of the POPI Act and other relevant
laws and regulations

Version 1.0 – September 2021

1. The JVR Africa Group

The JVR Africa Group of Companies includes JVR Psychometrics, JVR Consulting Psychologists, JVR Academy as well as JVR People Development Botswana and JVR Namibia. Youth development work is done through JVR4Youth. All the JVR companies process personal information as part of the products, learning material, and services they offer:

- JVR Psychometrics specialises in developing, validating, and combining psychological and other assessments for talent identification, talent development, and research purposes.
- JVR Consulting Psychologists uses assessments and consulting services to ensure optimal talent utilisation for small and large companies in the public and private sector.
- JVR Academy offers an extensive range of learning and development events in virtual-, blended- and in-person formats.
- JVR4Youth specialises in developing young talent and preparing them for the workplace.
- All the intellectual property required for processing of products, learning material, and services available within the broader JVR Africa Group are also available for work done in Namibia and Botswana.

In addition to the scientific and psychological expertise existing in the JVR companies, access to accurate, appropriate, verified, and relevant personal information is essential in embarking on the talent identification and talent development work contracted for by clients. In this regard JVR functions as Operator/Processor of personal information and professional expertise at the request of, and by agreement with a client.

Compliance to legislation is core to all JVR activities. Commitment to the Protection of Personal Information Act No. 4 of 2013 (POPIA), following the guidelines of the National Health Act No. 61 of 2003, the Health Professions Act No. 56 of 1974 (HPA), and the Health Professions Council of South Africa (HPCSA) guidelines and regulations are central to how personal information is managed in the work done by JVR.

In addition to South African legislation, JVR ensures compliance to the principles of the General Data Protection Regulations 2016/679 (GDPR) as established by the European Union and the European Economic Area.

2. JVR Measures and Protocols for Compliance

JVR have a vast number of measures and protocols in place to ensure the safeguarding and ethical management of personal information as is stipulated by the POPIA, HPCSA, GDPR, and other legislation. Some of these include:

2.1 Corporate Identity, Professional Registration, Values, and Culture

Since its inception, three decades ago, JVR employs psychologists and psychometrists registered and in good standing with the HPCSA. Many of these employees are in senior management. The principles of psychological ethics, regulations, and laws are embedded in the culture, values, policies, and in terms of the JVR disciplinary code. All of this serve to support compliance with regards to how personal data is managed.

2.2 HR Framework

A range of JVR Policies, reinforced with ongoing training, has been established in the following clusters:

- Board Policies and Documentation
- Protection of personal information (POPIA) Policies, including a policy on the alignment with GDPR
- Human Resources (HR) Policies
- Information Technology Policies
- Corporate Governance Policies
- JVR Terms of Business

The JVR Terms of Business, the Confidentiality, and Data Security Policies, and PAIA Manuals are public documents available on the JVR Africa website <https://jvrafricagroup.co.za/>. They can also be obtained by contacting the informationofficer@jvrafrica.co.za or contacting JVR during office hours at 27 11 781 3705/6/7.

2.3 Data Mapping and Information Life Cycle Analysis

The identification and management of all “data touchpoints” is an ongoing project to ensure the safety of personal data and information at all points of processing across the life cycle of the information.

2.4 Contracts, Agreements, and Third-Party Resources

Employment and third-party contracting are done with formal contracts and agreements specifying access, management, and limitations in the access, processing, and management of personal data.

2.5 Consent

The interaction JVR has with clients for the delivery of products, learning material, or services starts with a request for consent to be provided. Such consent specifies the purpose and use of personal information, and the client can “opt out” should they prefer to do so.

2.6 Data Retention and Destruction

The nature of data processed and retained by JVR is most often psychological in nature, and in this regard our compliance is with the HPA in addition to POPIA, where safe retention is specified for at least 6 years, allowing also for the anonymising the information. Where destruction of data can be done, it includes both paper-based and electronic formats of information.

2.7 Special Information of Vulnerable and Sensitive Population Groupings

JVR does, at time, work with vulnerable population groups such as children or people with disabilities. In this regard all work done is according to the principles of the HPCSA, POPIA, and GDPR guidelines.

2.8 Technical Controls

Information technology is core to the products and services offered by JVR. Care is taken with all the systems used by JVR to ensure the safety and security of personal data. JVR policies regarding Privacy and Security of Data and our Terms of Business are available on our website (<http://jvrafricagroup.co.za>). The JVR technology equipment, devices, and platforms are continuously monitored and reviewed to ensure the best security mechanisms, protocols, and incident management policies.

2.9 Cross-border Processing

The JVR electronic, technical, and online systems are, in some cases, integrated with other similar international systems. These integrations allow for the sub-processing of data - a function that is essential to the JVR business. In compliance with POPIA Section 72, equivalence in the Personal Information legislation is ensured before any sub-contracting.

2.10 Appointment of the Information Officer

JVR has registered an Information Officer and Deputy Information Officer with the South African Information Regulator. These senior staff members and the Board Committee supporting this role can be contacted for comments, information, or complaints by sending an email to the informationofficer@jvrafrica.co.za or phoning us during office hours at 27 11 781 3705.

2.11 Promotion of Access to Information Act (PAIA) Compliance

The PAIA Manuals for the respective South African companies within JVR have been compiled and are available on the JVR website <https://jvraficagroup.co.za/> and during office hours at the reception of the JVR Head Office (15 Hunter Street, Ferndale, Randburg).

2.12 POPI Act Operator Agreements

JVR enters into POPIA Operator Agreements with clients and service providers in compliance with article 21 of the POPI Act, which stipulates that a contract must be established between the responsible party (client) and the Operator (JVR) for the processing of personal information. The purpose is to clarify accountability, responsibilities, and conditions. The entering into of an Operator Agreement is a condition precedent for the entering into of every SLA.

2.13 Business Continuity

JVR has established comprehensive and safe measures to ensure the continuation of the business under all circumstances. These include the following:

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Business continuity council, consisting of all the company directors

The purpose of the above is to continuously manage and monitor all aspects for securing business safety and continuity, also including strategy, risk management, operations, and succession planning.

2.14 Risk Management

JVR has established risk management as a business discipline. This is continuously updated and monitored by the Boards of Directors. Information security is one of the key risk categories contained and mitigated through this process.

2.15 Marketing and Sales

JVR does not sell personal information. Only those clients who have indicated an interest or willingness to do business with JVR, have requested marketing information, or registered for our newsletter, receive information from us.

2.16 Physical Security

Measures and protocols have been established to ensure the physical safeguarding of the JVR

premises, as well as the contracting of such measures at the premises of suppliers and third parties who may have access to personal information which is processed by JVR.

3. Context for Compliance with the Laws for Protection of Personal Information

Since its establishment in 1993, the work done by JVR has involved sourcing, capturing, and safely storing personal information. The legislation and regulations guiding the sensitive and responsible management of such information have, before the publication of POPIA, always been the National Health Act No. 61 of 2003, the Health Professions Act, and the HPCSA guidelines and regulations on ethical and professional practice.

Whereas in the past, safeguarding personal information required specific attention to be given to the responsibilities of employees and the safe storage of printed material, current requirements include the safeguarding of personal information in technical and electronic systems and processes.

Compliance required to the South African POPIA, the HPCSA regulations, and ensuring adherence to the international GDPR legislation in a technologically oriented workplace, has led JVR to draft this Declaration. Specific attention is given not only to JVR's role and responsibilities as Operator/Processor, but also to the role and responsibilities of the client.

4. Purpose of this Declaration

The purpose of this declaration is to confirm:

- the role of JVR as an Operator/Processor of confidential personal information; and
- the responsibilities of both parties to adhere to requirements of the POPIA, GDPR, and HPCSA regulations.

The entering into of a POPIA Operator agreement is a condition precedent for a negotiated and signed Service Level Agreement (SLA) specifying the processing services required by the client.

5. Definitions

In this Declaration, unless the context indicates a contrary intention, the following words and expressions bear the meanings assigned to them:

“Client” means a person who requests and enters into an Operator Agreement as well as SLA with JVR to process personal information of their employees or third parties.

“Data subject” means the person to whom personal information relates.

“GDPR” means the principles of the General Data Protection Regulations 2016/679 as established by the European Union and the European Economic Area.

“HPA” means the Health Professions Act No. 56 of 1974, as amended from time to time.

“HPCSA” means the Health Professions Council of South Africa.

“Information Officer” of, or in relation to a:

- Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of POPIA; or
- Private body means the head of a private body as contemplated in Section 1 of PAIA.

“JVR” means the JVR Africa Group of companies or JVR Psychometrics (Pty) Limited, company Registration Number: 2001/015618/07, as the context may require.

“Operator” means a person who processes personal information for a client in terms of a contract or mandate, without coming under the direct authority of that party – in this case JVR.

“PAIA” means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) as amended from time to time.

“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:

- a. 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.
- b. Information relating to the education or the medical, financial, criminal, or employment history of the person.
- c. Any identifying number, symbol, email address, telephone number, location information, online identifier, or other particular assignment to the person.
- d. The biometric information of the person.
- e. The personal opinions, views, or preferences of the person.
- f. Correspondence sent by the person that would reveal the contents of the original correspondence.
- g. The views or opinions of another individual about the person.
- h. 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.

“POPIA” means the Protection of Personal Information Act (Act No. 4 of 2013) as amended from time to time, the South African data protection privacy law, which as its main function and objective, regulates and controls the processing of personal information by an operator on behalf of a client.

“Processing” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- a. The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.
- b. Dissemination by means of transmission, distribution, or making available in any other form.
- c. Merging, linking, as well as restriction, degradation, erasure, or destruction of information.

“Pseudonymisation” or “Anonymised data” means that personal data cannot be attributed to a specific data subject without the use of additional information kept separately and subject to “technical and organisational” measures.

“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 personal information – in this case the Client.

“SLA” means a Service Level Agreement between JVR and a Client, which sets out the services required by the Client of JVR.

6. Duties and Responsibilities of both Parties

As required by POPIA, each party shall:

- Accept and comply with its own obligations under POPIA.
- Maintain written security policies and measures that are fully implemented, trained on, and applicable to the processing of Personal Information.
- Implement and maintain all such technical and organisational security procedures and measures required to preserve the security and confidentiality of the Personal Information in its possession.
- Protect such Personal Information against unauthorised or unlawful disclosure, access, or processing, accidental loss, destruction, or damage.
- Provide, collect, use, store, process, and report on Personal Information to render the services or to comply with the obligations imposed/requested in terms of a mutually accepted SLA.

6.1 Duties and Responsibilities of the Client as Responsible Party

As required by POPIA, the Client shall:

- Enter into a POPIA Operator Agreement with JVR to benefit from the services of JVR as Operator/Processor to process personal information for the purposes set out in the SLA.
- Explicitly clarify, authorise, and agree upon the business purpose and expected output for which JVR as Operator will have access to the relevant Personal Information as provided.
- Guarantee that it has all necessary rights to provide the Personal Information to the Operator for the processing to be performed in relation to the services.

- Ensure that the request for processing is lawful and in compliance with POPIA, HPCSA, and other legislation.
- Make sure that all the Personal Information provided is personally verified, accurate, true, and relevant to the business processing contracted for.
- Take full responsibility for ensuring that all necessary communication, clarification, and privacy notices/assurances are provided to their own Data Subjects.
- Ensure that consent for the processing of Personal Information is obtained from the Data Subjects and that a record of such consent is safely maintained.
- Allow Data Subjects to revoke their consent and communicate this timeously to the Operator with relevant instructions with respect to the impact this may have on the contracted agreement for products, learning events, and services.

6.2 Duties and Responsibilities of JVR as the Operator/Processor

As required by POPIA and HPCSA regulations, JVR as Operator/Processor shall:

- Treat all Personal Information as confidential following POPIA, HPCSA, and GDPR guidelines and regulations when receiving, storing, processing, and disclosing Personal Information of data subjects in contract with and on behalf of the Client.
- Guard against unauthorised or unlawful access, processing, accidental loss, destruction or damage, alteration, disclosure, or access to Personal Information.
- Continuously inform its employees, agents, and/ or approved sub-Operators engaged in processing the Personal Information of the confidential nature of the Personal Information.
- Ensure that all such persons or parties sign confidentiality agreements and contracts, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.
- Ensure technical security by ensuring the integrity and resilience of the JVR processing systems, the implementation of secure passwords, using antivirus protection, doing secure backups, ensuring encryption and pseudonymisation of data, ensuring ongoing checks for vulnerabilities, and more. These measures are constantly evaluated and continuously improved.
- Only process Personal Information on receipt of consent and documented instructions of the Client to the extent that this is required for the provision of the services.
- Actively manage all comments, requests, and complaints received by the informationofficer@jvrafrica.co.za
- Notify and work with the Client to investigate, formulate a response, and take further remedial actions in respect of an incident (breach of security or confidentiality, receipt of complaint, accidental access, loss of information, or unlawful processing of Personal Information, etc.) that may have a material impact on the processing of the Personal Information of the Client that is the subject of the SLA.
- Be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes contracted for with the Client, provided that all such discretion is compatible with the requirements of the relevant legislation and the Client's written instructions.

- When using the services of national and international sub-Processors in the scoring or processing of Personal Information, ensure contractual agreements that require equivalence and compliance to the POPIA, HPCSA, and GDPR legislation regarding the safety and security of Personal Information.
- When/if required to disclose or process any Personal Information required by law, regulation, or court order, be guided by the principles of the HPA and POPIA. In this regard JVR will:
 - Advise the Client thereof prior to disclosure, if possible. If prior disclosure is not possible, the Operator shall advise the Client immediately after such disclosure.
 - Take such steps to limit the extent of the disclosure to the extent that is lawfully and reasonably practically possible.
 - Afford the Client a reasonable opportunity, if possible and permitted, to intervene in the proceedings.
 - Comply with the Client's requests as to the manner and terms of any such disclosure, if possible and permitted.
- Do research on anonymised and depersonalised Data in compliance with HPCSA and POPIA legislation and/or on contractual instruction of a Client if in compliance with legislation.
- Return processed Personal Information on request only to the Client who contracted, complied, paid, and provided the instruction for the processing.
- Comply with HPCSA regulations and legislation regarding the safekeeping of personal and processed data for at least 6 years.
- Upon termination of the agreement between JVR and the Client, or upon the Client's written request, or upon fulfilment of all purposes agreed in the context of the services whereby no further processing is required, the Operator can, at the written request of the Client, Anonymise/Pseudonymise the Personal Information.
- Assist Clients by making available information to demonstrate compliance with POPIA, and HPCSA legislation.

7. Duration and Termination

A POPIA Operator Agreement shall come into effect on the commencement date of the applicable SLA.

Termination or expiration of the POPIA Operator Agreement shall not discharge the Operator or the Client from its confidentiality obligations in terms of that agreement.

The Operator shall process Personal Information until the date of expiration or termination of the applicable SLA, unless instructed otherwise by the Client, or until such data is returned or anonymised on instruction of the Client.

8. Conflict

In the event of any inconsistency or conflict between the provisions of the POPIA Operator Agreement and the provisions of the applicable SLA, the provisions of the POPIA Operator Agreement shall prevail.

In the case of any inconsistency or conflict between the provisions of POPIA and the GDPR, the parties will adhere to the provisions of POPIA.

9. Laws

The POPIA Operator Agreement shall be governed by the laws of the Republic of South Africa. Any disputes arising from or in connection with the POPIA Operator Agreement shall be brought exclusively before a competent court in South Africa.

10. Information Officers

The Client shall supply the name, surname, contact number and email address of its information officer.

Contact information of the Information Officer of JVR as Operator/Processor:

Name and Surname: Dr Jopie de Beer

Contact number: 083 4477319/27 11 781 3705

Email address: informationofficer@jvrafrica.co.za

Date of issue: 6 September 2021

Status and Approval

VERSION	DATE	COMPILED BY	ACTION
1.0	6 September 2021	Dr J de Beer	1 st publication
	6 September 2021	E Rust	Language editing and proofreading