



THE JVR AFRICA GROUP

Privacy Policy

June 2021





JVR Africa Group Privacy Policy

The JVR Africa Group (JVR) holds privacy to be of primary importance in all its business practices. We are committed to the security, confidentiality, processing, integrity, and safeguarding of all personal information collected on all the JVR online platforms and electronic services. It includes JVR administrative tools, commercial websites, assessment portals, survey tools, talent management sites, e-learning sites, application products, and e-commerce sites. In essence, by visiting any of our JVR sites and using any of our electronic services, you are accepting the practices described in this Privacy Policy.

JVR's commitment to protecting and respecting privacy is done in compliance with current data protection legislation, including the Protection of Personal Information Act No. 4 of 2013 (POPIA), the General Data Protection Regulation (GDPR, EU 2016/679) as it relates to South African legislation, and the rules, regulations, and ethical principles of the Health Professions Council of South Africa (HPCSA). For further information regarding compliance specific to these elements or national and international law, please contact us at: +27 (0) 11 781 3705/6/7 during office hours or send an email to: informationofficer@jvrafrica.co.za

Structure of the Policy

This Privacy Policy sets out the way in which JVR ensures privacy in how data and information are collected, stored, used, managed, and updated.

Specific attention is given to issues such as:

- Collection of information
- Cookies
- Children
- Information and data security
- No information shared
- Opt-out
- Personal information alteration
- Retention of data
- Third party websites
- Transmission of information
- Web security
- JVR Privacy Policy changes
- Contact information

Collection of Information

At JVR, we use information received from clients to ensure excellence in the delivery of our services, assessments, training, learning solutions, and consulting processes. Our aim is to continuously improve our products and services, particularly also our online offering to clients. The information we rely on can be categorised as information provided to us by clients, and information obtained automatically.

Information provided by the client

We receive and store the information that you provide through interactions with us and when you enter information on our online platforms. The information can originate from forms that you complete when you open an account, order material, submit qualification criteria, request information, ask for quotes, do assessments, participate in consulting interventions, register for training, sign up for JVR events and promotions, or report a problem. The information required on these forms may include personal contact information (identity, data, and contact details), demographic and biographical information, financial and transactional data, product purchase history, and other essential information required for JVR's governance, business analytics, and the delivery of our assessment-, training-, and consulting services. We limit the use of the information obtained from you to the tasks required for governance, delivering the product(s) and service(s) requested, and the optimisation of our processes and services to our clients.

Some of our assessment and service sites may specifically collect information related to age, gender, race/ethnicity, education, and occupation when it is relevant to the services provided. When such personal information is submitted, it is processed for the purposes for which you have submitted it to us. You may choose not to provide certain information, however, your decision not to provide certain information may limit the use of the products and services available to you.

On occasion we collect a special category of data from respondents who take our questionnaires and surveys for research purposes. Such a special category data collection study is clearly communicated, and participation is optional and requires consent. The data is used in aggregated and anonymised form for research and product development purposes. No personal data will or can be disclosed since no person is identifiable from such data.

Information obtained automatically

The JVR websites obtain information that is automatically generated by a user's Internet Service Provider (ISP). This information may include the internet protocol (IP) address, domain types, the browser type used to access the JVR sites, the location of the ISPs' servers, the pages of the JVR sites that a user views during the visit, any search terms entered on the sites, the website address and email address of a user, and any other information transmitted by the user. This information may be collected for system administration purposes, to gather broad demographic information, to monitor the level of activity on the site, for technical support, and to improve the JVR websites by responding to customer/client interests and needs. JVR does not link IP addresses to personal information on our website. We do, however, reserve the right to link the IP addresses and other information supplied by the Internet Service Provider (ISP) to personally identifiable information if it is required to protect the integrity of our systems and for security purposes.

Cookies

Cookies are small text files that a website transfers to your computer's browser, which are used by many websites to perform a variety of functions, such as remembering your preferences, recording what you have put in your shopping basket, and counting the number of people looking at a specific website.

JVR websites use cookies to measure traffic patterns, to provide personalised content, and to control security. The information that cookies collect consists of non-personally identifiable information. To eliminate cookies stored on your computer, please follow your respective browser instructions.

The website uses a cookie for Cross-site request forgery protection and creates an X-XSRF-TOKEN in a user's browser. This is simply to provide an extra layer of protection against cyberattacks. It doesn't track users' personal data.

For the search Application Protocol Integration (API), JVR uses Algolia and more specifically, their search analytics feature. When a user makes a search request, two things are logged:

- Their IP address.
- Whole search request (query parameters, query, headers, etc.).

This data is processed internally by Algolia for services like monitoring and analytics (which sends weekly analytics reports on the terms people have searched for to the JVR webmaster, but not their identifying data like IP). Algolia deletes all logs after 90 days. JVR does not use the Algolia 'Click and Conversion Analytics', so no uniquely identifying attributes are collected.

JVR also uses the following services for the management of Cookies:

- Google Analytics to monitor and analyse interaction on the website. Google Analytics collects a vast majority of user data, including their IP address (which can be anonymised with adding a parameter to a piece of code if this is required), pages visited, time spent on pages, browser, and operating system, etc.
- Collects personal information via the marketing hub's forms, which saves their data in our CRM system, such as name, surname, phone number, and email address. We only use this to create leads and request appropriate consent for collecting this information.

No Information Shared

At JVR, we are committed to maintaining a healthy and trusted relationship with our clients and we value the information provided on all our online platforms. We do not share client information with third parties for purposes outside the scope of the products and services we provide. We will not release, sell, or distribute personal information to any third party, unless it is required to do so by law, in the course of a merger or acquisition, or with consent from the individual to whom the personal information pertains. We do not share, sell, or rent any personal information to third parties for promotional use. We may, however, at our sole discretion disclose information to protect JVR or third-

party property rights, should the information be essential for the public or safety of an individual, and to prevent or stop any illegal, unethical, or legally actionable activity, to comply with the law, or comply with a lawful request by public authorities, such as may relate to national security or law enforcement requirements.

Information and Data Security

We strive to protect the security of information using Secure Sockets Layer (SSL) software, which encrypts information on the protected sites where information is provided. For secure data transmission between websites, the latest Transport Layer Security (TLS) protocol is used, which works with the most current web browsers, encrypting information exchanged over a network, and protecting against disclosure to third parties.

How we keep your data secure

At JVR, we are concerned about safeguarding the confidentiality of personal information. In this regard we ensure the security and integrity of personal information through a variety of industry standard security measures which include administrative, physical, technical, and organisational procedures and measures. This is to ensure the protection of personal information from unauthorised access, use, disclosure, and possible misuse. These integral measures are consistently reviewed and updated to ensure the security and protection of all personal information.

Our IT infrastructure and applications are built to provide secure deployment of our products and services, encrypted storage of backup data with end user privacy safeguards, encrypted communications between services, and safe operations by clients.

Our staff, associates, and consultants are bound to comply with confidentiality provisions and privacy statements, in addition to completing mandatory privacy and data protection training. We have numerous policies that specifically address responsibilities and expected behaviour with respect to the protection of confidential information.

Respondent data is only available and accessible by selected JVR employees that support and administer the scoring- and report-generation systems, including our web-based scoring and delivery platform. Respondent data is accessed on a need-to-know basis only.

We have procedures for incident management and breach investigation and notification. Where our impression of the likely risk to the individuals involved concludes that a breach of personal data may result in risk to the rights and freedom of individuals, we shall promptly inform the individuals and legal authority of such a breach, as is required by law and in accordance with any contractual terms.

When you sign up to use our online platforms, we provide you with a username and password that enables you to access certain parts of the online services, account information, recent purchases, or products and services. These passwords provide limited rights, such as accessing, reviewing, and updating information only. All payment transactions are processed directly by the JVR Accounts Department and through a gateway provider, and credit card information is not stored or processed on any of our servers.

You are urged to also take personal responsibility for protecting yourself against unauthorised access to your access information and passwords on your personal account and computer. Be sure to sign off when finished working on any of our online systems, particularly when using a shared computer.

Retention of data

At JVR, we keep personal information for as long as it is required to fulfil the purposes for which it was collected and as required by law.

We are bound by South African legislation (The Health Professions Act No. 56 of 1974) to keep psychological test data for a minimum of five to seven years. Such data is securely archived. We only retain your current personal data for as long as it is necessary to fulfil the purposes for which the data is collected, including for the purposes of satisfying the needs of legal, organisational, third party, accounting, or reporting requirements. Thereafter it is archived. The periods for which we retain specific data are set out in our POPI Policy: *Data Retention and Destruction*.

Web Security

JVR websites are protected by the Transport Layer Security (TLS 1.2) encryption protocol and are secured to ensure that users are browsing our websites in a secure manner. We utilise security measures consistent with current best practices to protect its websites, email, and mailing lists. Although no transmission over the internet can be guaranteed to be absolutely, secure we are committed to protecting all personal data and any information transmitted to us.

Third-party websites

Please note that JVR bears no responsibility for the privacy policies and practices of websites that may be linked to any JVR website or to companies that may provide additional products or services. Please refer to those organisations' specific privacy policies to learn how they collect, use, and disclose information.

Transmission of Information

Data collected and received by JVR in connection with the delivery of assessments, training services, and consulting interventions is transmitted and stored with a third-party Cloud Services Provider (CSP). The internet is a global environment, and by using our sites and sending information to JVR electronically you consent to transborder- and international transmission of any personal information collected or processed through our sites.

Data and Personal Information Transfer

Scoring

For the purposes of scoring assessments, JVR may share assessments, responses, and limited personal information with third parties, some of whom may be located outside South Africa. Such processing functions are managed by national and international companies who comply with POPIA (nationally) and GDPR legislation (internationally). We remain vigilant that such compliance remains.

Data collected and received by JVR in connection with the delivery of assessments will be transmitted and stored in South Africa, in some cases the United States or Australia, and in certain circumstances in Europe, with a third-party Cloud Service Provider (CSP).

Where personal data is transferred outside South Africa, we take all reasonably necessary steps to ensure that your data is transported securely and in accordance with this privacy policy and the requirements of the law. Such measures include, where applicable, ensuring that recipients of the data are within countries where the European Commission has made an adequacy decision with respect to the data protection laws of such country.

Releasing reports

At JVR, we share your data in the form of report output with the practitioner who is duly qualified, professionally registered, or appointed to work with the assessment or report output data. Such a qualified party is professionally and legally bound to working with your results in an ethical, confidential, and legally compliant manner.

The practitioner may also share the results (or a summary thereof) with another practitioner or professional services team that is involved in the process that uses the assessment results, provided that you are informed that this will occur and that you have agreed by providing written consent.

Alteration of Personal Information

Please note that you can always choose not to provide information to JVR, although this could impact on our ability to provide products and services. In the event that you require your personal information to be updated, changed, transferred, deleted, or removed, this request needs to be made to the JVR Information Officer (informationofficer@jvrafrica.co.za) or call +27 11 781 3705/6/7 during office hours. It should be noted that removing and deleting information may take a reasonable time and you could incur costs for the request.

Opt-out

Since the majority of JVR communication is conducted via email, you have the option to unsubscribe from any email correspondence or listings, and in doing so will no longer receive any further email communications. We also allow data subjects or respondents to opt out of JVR assessment- and services

site links at any time after they have initiated the assessment process. Doing so may however impact on JVR or a professional's ability to provide the required products and services.

Children

We do assess and provide e-learning and various services for children. Confidentiality of their information is managed according to all legal specifications, specifically also the best practice guidelines and ethics of the HPCSA and the POPIA.

Changes to JVR Privacy Policy

JVR reserves the right to make changes to its privacy policy without prior notice. Regular reviews and updates to this policy are made from time to time to reflect changes consistent with industry best practices, legislation, professional standards, and the JVR policies. We encourage you to review this *Privacy Policy* periodically for any changes and updates.

Contact Information

If you have any questions or concerns regarding this *Privacy Policy*, please contact the JVR Information Officer at: informationofficer@jvrafrica.co.za

Security and Privacy

Please note that the JVR data security protocols are formulated in our Security and Privacy Policies available on the JVR systems site. This document should be read in conjunction with these- and all the other JVR Terms of Business Policies available on this site.