

R2K NEXUS (PTY) LTD

PRIVACY NOTICE

Website, meeting requests and HAZMAT R2K services

Last updated and effective	5 January 2026
Responsible party	R2K Nexus (Pty) Ltd Registration number 2025/012935/07 VAT number 4130321484
Business address	56 Italian Road, Newlands, Johannesburg, Gauteng, 2092, South Africa
Privacy contact	Information Officer / Privacy Enquiries edwardvdw@r2knexus.co.za

IN PLAIN LANGUAGE: We collect only the Personal Information reasonably needed to respond to you, provide and secure the HAZMAT R2K services, administer Customer relationships, meet legal obligations and communicate about our services. We do not sell Personal Information. Meeting-form submission does not subscribe you to marketing.

This Privacy Notice (also referred to as our Privacy Policy) explains how R2K Nexus processes Personal Information under the Protection of Personal Information Act 4 of 2013 (POPIA). It should be read with our Service Terms, any Customer-specific services proposal or data processing agreement, and the live cookie notice where applicable.

• Scope and application

This Notice applies to Personal Information processed by or for R2K Nexus through www.r2knexus.co.za, contact and meeting-request forms, business communications, sales and support activities, Customer administration, and the HAZMAT R2K hosted platform and related professional, maintenance and managed services.

It applies to website visitors, people who contact us, prospective and current Customer representatives, suppliers, business partners, authorised platform users, and employees or contractors whose Personal Information a Customer submits to or generates within the HAZMAT R2K services.

This Notice does not replace a Customer's own employee, workplace or applicant privacy notices. A Customer remains responsible for explaining its own processing, workplace monitoring, access decisions and statutory obligations to its personnel.

A third-party website, social platform or service linked from our website has its own privacy terms. This Notice does not govern that third party's independent processing.

• Key terms

Authorised User: a person whom a Customer authorises to access the HAZMAT R2K platform.

Customer: an organisation that obtains or evaluates R2K Nexus services, including an employer that gives its personnel access to HAZMAT R2K.

Customer Personal Information: Personal Information submitted to, stored in or generated through the services on a Customer's behalf.

Data subject: the person to whom Personal Information relates.

Operator: a person who processes Personal Information for a responsible party under a contract or mandate, without being under that party's direct authority.

Personal Information: information relating to an identifiable living natural person and, where POPIA applies, an identifiable existing juristic person. It includes contact details, identifiers, online identifiers, employment-related information, correspondence and opinions.

Processing: any operation concerning Personal Information, including collecting, recording, organising, storing, using, sharing, restricting, deleting or destroying it.

Responsible party: the person that determines the purpose of and means for Processing Personal Information.

Services: the HAZMAT R2K platform and the related implementation, professional, support, maintenance, SDS mobilisation, document-management and managed services supplied by R2K Nexus.

• Who is responsible for the information

R2K Nexus is the responsible party when it determines why and how Personal Information is processed for its website, meeting and contact requests, sales, Customer and supplier administration, billing, security, support, service improvement and its own legal obligations.

For Customer Personal Information processed within HAZMAT R2K on a Customer's documented instructions, the Customer ordinarily acts as the responsible party and R2K Nexus ordinarily acts as its operator. The facts and applicable law determine the roles, regardless of the labels used.

When acting as an operator, R2K Nexus processes Customer Personal Information with the Customer's knowledge or authorisation, under the services agreement and any data processing agreement. R2K Nexus may still act as a responsible party for related account security, billing, fraud prevention and legal records where it independently determines those purposes.

If a privacy request concerns Customer-controlled information, we may refer the request to the relevant Customer and assist it as required by our agreement and POPIA.

• Personal Information we may collect

The exact information depends on how you interact with us and which services the Customer enables.

Context	Examples of information	Why it is relevant
Contact and meeting requests	Name, organisation, job title, work email, telephone number, preferred date and time, time zone, subject, message and communication history.	To respond, qualify the request, arrange a meeting and keep an appropriate business record.
Customer and supplier administration	Business contact details, authority, contract, quotation, purchase-order, invoice, VAT, payment-reference and procurement information.	To form and administer relationships, invoice, receive payment, maintain records and manage suppliers.
Accounts and access	Name, work email, employer, site, department, role, user identifier, permissions, account status and authentication or recovery information.	To create accounts, control access, support users and maintain accountability.
HAZMAT R2K workplace records	Where enabled: employee or contractor name, role, site, chemical or SDS access, acknowledgement, assignment, training-related status, action ownership, review activity and audit history.	To help the Customer provide access to current hazard information, assign responsibility and evidence relevant actions.
Chemical and SDS content	Chemical register and inventory details, SDSs, suppliers, locations, issue and review dates, document status, classifications and responsible-person details. Much of this is business or safety data rather than Personal Information.	To provide the core document, review, notification, search and reporting functions of HAZMAT R2K.
Support and communications	Support tickets, email content, call or meeting notes, attachments, feedback, fault details and resolution history.	To answer questions, troubleshoot, improve delivery and evidence instructions or resolution.
Technical and security data	IP address, browser and device information, dates and times, session and access logs, referring page, approximate region, error logs, security events and bot-detection or challenge results.	To operate, diagnose and secure the website and services, prevent abuse and maintain auditability.

Context	Examples of information	Why it is relevant
Transactional email	Sender and recipient details, message content and identifiers, delivery status, bounce or complaint information and delivery logs.	To deliver meeting requests, automatic confirmations, account messages, alerts, support replies and other service communications.
Preferences and marketing	Consent or objection status, communication preferences, subscription source and engagement with permitted marketing messages.	To honour choices and communicate lawfully about relevant R2K Nexus services.

Please do not place passwords, full payment-card details, identity documents, medical information, exposure records or other special Personal Information in an open meeting or contact form.

Unless a services proposal and data processing arrangement expressly cover it, Customers must not submit children's information, medical records, biometric information or other special Personal Information to HAZMAT R2K.

• Where we obtain Personal Information

We may collect Personal Information directly from you when you use a form, communicate with us, attend a meeting, enter into a business relationship, create or use an account, request support, make a payment or select communication preferences.

We may receive it from your employer or another Customer, a Customer administrator, an authorised colleague, a supplier or business partner, or a person arranging a meeting or service on your behalf.

We may generate it through use of the website or services, including access history, audit records, security events, service alerts and delivery logs.

Where lawful and relevant to a business relationship, we may obtain professional contact information from public company websites, professional directories, public records, event organisers or reputable business-information providers.

If you provide Personal Information about another person, you must be authorised to do so and must make this Notice available to that person where reasonably practicable.

• Why and when we process Personal Information

POPIA permits Processing in several circumstances. Depending on the context, we process information with consent; to conclude or perform a contract; to comply with law; to protect a legitimate interest of the data subject; or to pursue the legitimate interests of R2K Nexus, a Customer or a third party, provided those interests do not unjustifiably override the data subject's rights.

Purpose	Typical Processing	Typical justification
Respond and arrange meetings	Receive the request, assess its subject, contact you, schedule the meeting and send a confirmation.	Your request; steps toward a contract; and legitimate business interests.
Provide and administer services	Set up Customers and users, deliver platform functions, professional or managed services, support, reporting and communications.	Contract, Customer instructions and legitimate interests in reliable delivery.
Support workplace hazard communication	Make relevant chemical and SDS information accessible, assign actions, track reviews or acknowledgements and produce audit history as configured.	Customer instructions, contract, workplace-safety interests and applicable legal duties.
Security and abuse prevention	Authenticate users, log access, detect malicious activity, validate Turnstile results, rate-limit requests, investigate incidents and protect availability.	Security duties, legitimate interests and protection of users and Customers.
Transactional communications	Send confirmations, account messages, alerts, password or access messages, support replies and delivery-status notices.	The underlying request or contract and legitimate interests in reliable communication.

Purpose	Typical Processing	Typical justification
Billing and administration	Prepare quotations, contracts and invoices; manage payments, tax and procurement records; and communicate with Customer or supplier contacts.	Contract, legal obligations and legitimate business interests.
Improve and govern services	Diagnose errors, measure reliability, manage quality, develop functionality and create de-identified statistics or trends.	Legitimate interests, contractual delivery and, for optional tracking, consent where required.
Marketing	Send permitted information about R2K Nexus's own relevant services and record preferences or objections.	Consent or the limited existing-customer circumstances permitted by POPIA section 69.
Legal, regulatory and claims	Meet statutory duties, respond to lawful requests, enforce agreements, obtain advice, preserve evidence and establish or defend rights.	Legal obligations and legitimate interests in compliance and claims.

We will not use Personal Information for a materially incompatible purpose without taking the steps required by POPIA, which may include giving further notice or obtaining consent.

• Whether information is voluntary or mandatory

A field is mandatory when it is marked as required, when law requires the information, or when it is reasonably necessary to perform a requested service, create or secure an account, administer a contract or respond to a request.

If required information is not supplied, we may be unable to submit or answer a meeting request, create or support an account, verify authority, secure access, provide the relevant service, complete a transaction or comply with law.

Marketing consent and optional profile or preference fields are voluntary. Refusing marketing does not prevent service or transactional communications.

• Meeting-request form, Resend and automatic confirmations

When you submit a meeting request, R2K Nexus uses the information entered in the form to deliver the request to the appropriate internal recipient, assess and respond to it, arrange the meeting and send an automatic confirmation to the email address supplied.

We use Resend as the transactional email delivery provider. Resend may process email addresses, names, message content, message identifiers, delivery events, bounces, complaints and related logs as needed to transmit and secure the messages.

Resend's data processing terms state that its primary processing operations take place in the United States and that it may use authorised subprocessors. R2K Nexus uses contractual and other appropriate safeguards for relevant cross-border Processing as described in clause 12.

Submitting a meeting request does not add you to a marketing list. Any marketing choice must be presented separately and must not be required to request a meeting.

Do not include unnecessary confidential, medical, identity, financial or other sensitive information in the free-text message field. If sensitive information is genuinely required, ask us for an appropriate secure channel.

• Cookies and similar technologies

The website and platform may use cookies, local storage, pixels, scripts and comparable technologies. Some are strictly necessary for navigation, sessions, security, load management, user preferences, accessibility and requested functions.

Cloudflare Turnstile is used on relevant forms to help distinguish legitimate visitors from automated abuse. It processes browser and security signals needed for that function, such as technical characteristics and challenge results. Cloudflare states that Turnstile does not access, store or transmit form entries, page inputs or user communications.

Optional analytics, performance or marketing technologies may be enabled only after they are properly configured, identified in the live cookie notice or preference tool, and handled with consent where applicable. The cookie notice should identify the provider, purpose and expected duration of each non-essential technology.

You may use the website's cookie controls, where available, and browser settings to reject or delete non-essential cookies. Blocking strictly necessary technologies may prevent a form, login or security feature from working.

We do not treat cookie consent as consent to unrelated direct marketing. A separate marketing choice is required where POPIA requires it.

• When we share Personal Information

We may disclose Personal Information only where reasonably necessary for an authorised purpose, subject to confidentiality, security and legal requirements. Recipients may include:

- R2K Nexus personnel and authorised contractors who require it for sales, service delivery, support, finance, security, compliance or management;
- the relevant Customer, its authorised administrators, your employer or another organisation through which you use the services;
- technology providers supporting website hosting, cloud infrastructure, databases, identity, monitoring, backup, security, communications and support;
- Resend for transactional email delivery and Cloudflare for Turnstile security checks;
- approved implementation, development, maintenance and managed-service providers acting under appropriate obligations;
- banks, payment, accounting, audit, insurance and professional-advisory providers;
- regulators, law-enforcement bodies, courts or other persons where disclosure is required or permitted by law, or reasonably necessary to protect rights, safety and systems; and
- a prospective purchaser, investor or successor in a genuine corporate transaction, subject to appropriate confidentiality and only to the extent reasonably necessary.

We do not sell or rent Personal Information. We do not disclose contact details to unrelated third parties for their independent direct marketing without a lawful justification.

Operators and service providers must process Personal Information for authorised purposes and protect it under written agreements where POPIA requires. We review material providers and may replace them as technology and service arrangements change.

• Material technology providers

Provider/category	Purpose and information	Location and safeguards
Resend	Transactional email delivery; recipient and sender details, message content and metadata, delivery, bounce and complaint events.	Primary processing in the United States according to Resend's DPA; authorised subprocessors may process elsewhere. Contractual and POPIA section 72 safeguards apply.
Cloudflare Turnstile	Form abuse and bot prevention; browser, device and challenge/security signals. Turnstile does not receive the form entries themselves according to Cloudflare's documentation.	Cloudflare may use global infrastructure. Contractual, security and POPIA section 72 safeguards apply where Personal Information is processed outside South Africa.

Provider/category	Purpose and information	Location and safeguards
Website hosting and deployment	Serve the website, handle requests, logs, availability and security. The exact provider depends on the production deployment.	The current provider and region are maintained in R2K Nexus's operator and privacy records. Cross-border safeguards apply where relevant.
HAZMAT R2K cloud and support providers	Host and operate platform data, databases, identity, monitoring, backup, support and managed services as contracted.	Locations and safeguards depend on the Customer environment and services proposal. A Customer-specific data processing agreement may provide more detail.

A current list of material operators or subprocessors relevant to a Customer may be requested using the contact details in clause 23. A signed data processing agreement may set notification or objection arrangements for provider changes.

• Cross-border Processing

Some providers and their subprocessors may process or store Personal Information outside South Africa, including in the United States and other countries in which they or their infrastructure operate.

R2K Nexus will make a cross-border transfer only where permitted by section 72 of POPIA or other applicable law. Depending on the transfer, safeguards may include a recipient subject to an adequate law, a binding agreement requiring substantially similar protection, appropriate contractual safeguards, consent, or a transfer necessary for a contract or requested pre-contractual step.

Foreign laws and enforcement practices may differ from South African law. We assess material transfers, require appropriate protection from providers and apply reasonable security controls, but we cannot represent that every foreign legal system is identical to POPIA.

A Customer-specific services proposal or data processing agreement may identify agreed hosting regions, transfer mechanisms and subprocessors more precisely and will prevail for its subject matter.

• Customer administrators and workplace visibility

If your employer or another organisation provides your HAZMAT R2K access, that Customer controls the account relationship and usually determines the relevant purposes, user roles, permitted records and retention.

Depending on configuration and permissions, Customer administrators and authorised managers may see your profile, employer, site or department, role, permissions, account status, SDS or chemical assignments, access or acknowledgement history, action ownership, review activity, support requests and audit records.

Customers must provide appropriate employee or contractor privacy notices, limit access to people who need it, keep information accurate, and use platform information lawfully. HAZMAT R2K supports compliance and employee access to hazard information; it is not intended for covert employee monitoring or unrelated performance profiling.

Questions about a Customer's workplace purpose or decision should be directed to that Customer. R2K Nexus will provide reasonable operator assistance where required.

• Retention and deletion

We retain Personal Information only for as long as reasonably necessary for the authorised purpose, a contract, security and evidential needs, legal claims or a period required or permitted by law. We then delete, destroy, de-identify or restrict it, subject to secure backup cycles and legal holds.

Record category	Normal retention approach
Meeting requests and ordinary sales enquiries	Up to 24 months after the last meaningful interaction, unless a Customer relationship begins, consent supports longer retention, a shorter period is appropriate, or law or a dispute requires longer.

Record category	Normal retention approach
Customer, supplier, contract, invoice and tax records	For the relationship and the applicable statutory or claims period. Tax and related commercial records are commonly retained for at least five years where South African law requires, and some records may require longer.
Platform accounts and Customer Personal Information	For the service term and the export, return, deletion and backup periods in the services agreement or data processing agreement. Standard post-termination export and deletion arrangements may be stated in the Service Terms.
Support and transactional email records	For as long as needed to resolve the matter, evidence delivery or instructions, maintain security and meet contract or legal requirements; normally no longer than 24 months unless linked to an active relationship, incident, dispute or mandatory record.
Security, access and audit logs	For a period proportionate to operational, security and audit needs; normally up to 24 months unless a Customer agreement, investigation, incident, legal hold or law requires longer.
Marketing preferences	Until consent is withdrawn or an objection is received. A minimal suppression record may be retained afterwards so that we continue to honour the opt-out.
Backups	Protected and removed or overwritten through controlled backup cycles. Information is not restored for ordinary use after deletion unless needed for disaster recovery, security or law, and any restored information remains subject to the applicable retention rule.

A Customer may lawfully instruct a different retention period for Customer Personal Information. We may retain a restricted copy where required for proof, a dispute, a security investigation or law, and will prevent unrelated use.

• Information security and security compromises

R2K Nexus uses appropriate, reasonable technical and organisational safeguards designed to protect the integrity and confidentiality of Personal Information and reduce risks of loss, damage, unauthorised destruction, unlawful access or unlawful Processing.

Safeguards may include role-based access, least-privilege administration, authentication controls, encryption in transit and where appropriate at rest, secure configuration, logging, monitoring, backups, vulnerability and patch management, confidentiality obligations, provider due diligence, incident response and periodic review.

Customers and users must also protect credentials and devices, use appropriate roles, remove access promptly, avoid sharing accounts, use supported software and notify R2K Nexus promptly of suspected compromise or misuse.

No internet-connected service or transmission can be guaranteed completely secure. This statement does not reduce our duties under POPIA or an applicable agreement.

Where there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person, R2K Nexus will investigate and issue or support notifications to the Information Regulator, affected data subjects and Customers as required by POPIA and the parties' roles. Notifications will be made as soon as reasonably possible, subject to lawful investigation needs.

• Your rights and choices

Subject to POPIA, PAIA and any lawful limitation, you may ask R2K Nexus to:

- confirm whether we hold Personal Information about you and provide access to it;
- correct or update information that is inaccurate, incomplete, excessive, out of date, misleading or obtained unlawfully;
- delete or destroy information that we are no longer authorised to retain;
- restrict Processing while accuracy, lawfulness or a request is being assessed where applicable;
- record and act on a lawful objection to Processing based on relevant legitimate interests;
- withdraw consent for future Processing where consent is the applicable justification;

- stop direct marketing and record your opt-out; and
- explain an applicable solely automated decision that produces legal or similarly substantial effects and provide an opportunity to make representations, where POPIA requires.

To exercise a right, contact the Information Officer using clause 23 and describe the information, relationship and requested outcome. We may ask for reasonable proof of identity or authority to protect the information. We will not request more identity information than reasonably necessary.

Some rights are not absolute. We may retain or withhold information where law permits or requires, including to protect another person's rights, legal privilege, confidential commercial information, security, evidence or a legal claim. We will explain a lawful refusal where required.

Formal access requests may be handled under POPIA and the Promotion of Access to Information Act 2 of 2000 (PAIA), including any prescribed form or fee. Our PAIA Manual should be consulted where applicable.

If the information is controlled by a Customer, contact that Customer first where practical. We will route or assist the request in accordance with our role and agreement.

• **Direct marketing and service communications**

We send unsolicited electronic direct marketing only with consent or in the limited existing-Customer circumstances permitted by section 69 of POPIA. A request for consent may be made only as permitted by law.

Every direct marketing message must identify the sender and provide a simple, free way to object or unsubscribe. You may opt out at any time. We will act on the request and may keep a minimal suppression record.

Meeting confirmations, account and security messages, password or access communications, service alerts, support replies, invoices and notices required for a contract are transactional or service communications, not marketing. You may not be able to opt out of communications necessary to provide or secure an active service.

We do not combine a required meeting or service submission with compulsory newsletter consent.

• **Automated Processing and decision support**

Cloudflare Turnstile automatically evaluates technical and browser signals to help determine whether a form submission appears legitimate. A failed or expired check may prevent online submission, but it is not used by R2K Nexus to make a decision with legal or similarly substantial effects about a person. If the form fails, you may contact us using clause 23.

HAZMAT R2K may generate reminders, status indicators, classifications, review dates, alerts, assignments, dashboards or audit outputs from configured rules and available data. These features support human action and safety governance; they do not replace the authoritative supplier or manufacturer SDS, workplace verification, a competent person's judgement or an employer's legal duties.

R2K Nexus does not intend to make decisions producing legal or similarly substantial effects about individuals solely by automated Processing. A Customer that configures or uses service outputs to make its own employment or workplace decisions is responsible for ensuring that use is lawful and appropriately explained.

• **Special Personal Information and children's information**

Our public website and meeting form are not intended to collect special Personal Information or children's information, and the services are intended for business and occupational use by adults.

Do not submit health, medical-surveillance, exposure, disability, biometric, criminal, trade-union, religious, political or children's information unless R2K Nexus has expressly agreed in writing that the service will process

it and the responsible party has established a lawful justification, necessary safeguards, access controls and notices.

If we receive such information unexpectedly, we may restrict, return or securely delete it where lawful and appropriate.

• De-identified and aggregated information

We may de-identify and aggregate information so that it cannot reasonably identify a person, Customer, site or confidential record. Properly de-identified information may be used for service reliability, security, research, statistics, benchmarking and improvement.

We do not attempt to re-identify information that has been irreversibly de-identified, and we apply safeguards against unauthorised re-identification.

• External links and social platforms

Our website or communications may link to third-party websites, manufacturer or supplier resources, standards, maps, videos or social-media platforms. The third party determines its own Processing and privacy terms. Review those terms before providing information.

If you communicate with R2K Nexus through a social platform, we may receive the information you choose to make available, including your public profile, handle and message. The platform also processes information independently under its own terms.

A link does not mean that R2K Nexus controls or endorses the third party's privacy practices. Please report a suspicious or broken link to us.

• Changes to this Notice

We may update this Notice to reflect legal, operational, provider or service changes. The current version will be posted on our website with its last-updated date.

Where a change materially affects how we process existing Personal Information, we will take reasonably practicable steps to provide additional notice and obtain consent if required. Changes do not retrospectively authorise unlawful or materially incompatible Processing.

A Customer-specific agreement or data processing agreement may require additional notice for changes to subprocessors, locations or Processing.

• Contacting R2K Nexus and lodging a complaint

Questions, privacy requests, objections and complaints should be sent to:

Organisation	R2K Nexus (Pty) Ltd
Attention	Information Officer / Privacy Enquiries
Email	edwardvdw@r2knexus.co.za
Address	56 Italian Road, Newlands, Johannesburg, Gauteng, 2092, South Africa

We encourage you to contact us first so that we can investigate and try to resolve the matter. You also have the right to lodge a complaint with the Information Regulator (South Africa):

General enquiries	enquiries@inforegulator.org.za
POPIA complaints	POPIAComplaints@inforegulator.org.za
Telephone	0800 017 160 (toll free) 010 023 5200

Address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
Website	https://infoeregulator.org.za

• General

This Notice is governed by South African law. It describes our intended privacy practices but does not create a right to process information where POPIA or another law prohibits it.

If a specific privacy notice, services proposal or signed data processing agreement applies to a particular Processing activity, the more specific provision will govern that subject matter to the extent of a genuine conflict.

A reference to POPIA includes its regulations, binding codes and lawful regulatory requirements, as amended or replaced.

INTERNAL IMPLEMENTATION APPENDIX

Concise notice for the website meeting form

This appendix is an implementation aid and is not part of the public Privacy Notice. Place the concise notice directly below the form fields and above the submit button, with "Privacy Notice" linked to the full notice:

By submitting, you ask R2K Nexus (Pty) Ltd to use your details to respond to and arrange your meeting. We use Cloudflare Turnstile to prevent form abuse and Resend to deliver the request and automatic confirmation. Your information may be processed outside South Africa under appropriate safeguards. Required fields are needed to respond. Submission does not subscribe you to marketing. See our Privacy Notice.

Form implementation requirements

- Link "Privacy Notice" to the published full notice and open it without losing the entered form data.
- Do not use a required "I agree to the Privacy Policy" checkbox merely to acknowledge ordinary Processing. Display the notice before collection. Use a separate, unticked checkbox only if optional marketing consent is requested.
- Mark mandatory fields clearly and collect only information genuinely needed to respond and schedule the meeting.
- Keep the free-text field warning: "Please do not include medical, identity, payment or other sensitive information."
- Validate the Turnstile token on the server before sending email; do not expose the Turnstile secret key or Resend API key in browser code.
- Send the internal request and confirmation through the verified R2K Nexus sending domain, and do not put the visitor's email address in the From field. Use Reply-To for the visitor where appropriate.
- Apply rate limits, server-side validation, logging that avoids unnecessary form content, and a clear fallback contact method when submission fails.
- Ensure the live cookie notice accurately lists any analytics, marketing, embedded media or other non-essential technologies actually deployed.