

Privacy Policy & Collection Notice - VOI Subjects

Scantek Solutions Pty Ltd (“**Scantek**” or “**We**”) collects information about you to be able to verify your identity on behalf of our client. Your privacy is important to us.

This Privacy Policy and Collection Notice (**Policy**) includes:

Privacy Policy & Collection Notice - VOI Subjects	1
Collection and Use of Personal Information	2
Why is your personal information being collected?	2
What personal information we collect and how we collect it	3
How we use your personal information	4
How will the Attorney-General’s Department handle your personal information?	5
How will the document issuer handle your personal information?	5
Security and storage	6
What happens if you don’t consent to providing personal information?	6
When we may share your information	6
Limited circumstances we may send personal information to overseas recipients	7
Unsolicited personal information and de-identification	8
Third Party Platforms	8
The Attorney-General’s Department’s verification assistance service	8
Integrity and retention of Personal Information	9
Request for Correction of Personal Information	10
How long we keep your personal information	10
General Privacy Related Information	11
Collection and Use of Non-Personal Information	11
Cookies and Other Technologies	11
Complaints	12
Children	13
Privacy Questions	13
Our Company Wide Commitment to Your Privacy	13

Scantek considers itself an Australian Privacy Principle (APP) entity and as such is committed to handling personal information in accordance with applicable privacy laws and complying with the *Privacy Act 1988* (Cth) (**Privacy Act**), the *Identity Verification Services Act 2023* (Cth) (**IVS Act**), the *Identity Verification Services Rules 2024* (Cth) (**IVS Rules**) and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)

(**AML/CTF Act**) where Scantek's services are provided in an AML/CTF compliance context, and to the implementation of practices, procedures and systems that ensure compliance with the Australian Privacy Principles and all relevant registered APP codes. We are bound by the provisions of the Privacy Act, including the Australian Privacy Principles (**APPs**), as well as the IVS Act, the IVS Rules and our Document Verification Services (**DVS**) Participation Agreement with the Commonwealth Government. Your personal information will be handled in accordance with our obligations under the above legislation and agreement.

If individuals have any specific needs or require this notice in an alternative format, or if you need assistance due to any special circumstances, please contact us.

In certain arrangements, Scantek provides verification of identity (**VOI**) and related identity verification services to third-party compliance platforms as an outsourced service provider. Where Scantek's services are accessed via such platforms, the platform is responsible for the primary collection notice provided to you covering the broader compliance workflow.

Collection and Use of Personal Information

Why is your personal information being collected?

Personal information is data that can be used to identify or contact a single person or information or an opinion about an identified individual, or an individual who is reasonably identifiable. In the context of the DVS, it also includes the outcome of a comparison involved in a DVS request.

Scantek generally collects personal information under four scenarios:

1. Information from Scantek's clients and potential clients (**Clients**) and their approved agents (including Client employees) for the purposes of establishing and maintaining a contractual arrangement with the Client and providing services to the Client;
2. Information from individuals whose identity is being verified (**Users**) by Scantek, generally on behalf of a Client;
3. Contact information for a User collected from a Client in order to facilitate the verification of identity (**VOI**); and
4. Information received from third-party compliance platforms (**Platforms**) that engage Scantek as an outsourced VOI service provider in connection with AML/CTF compliance, customer onboarding, or other regulated workflows. In these circumstances the Platform initiates the VOI on behalf of a reporting entity (such as a conveyancer, law firm, or financial services business). The Platform will generally

have already provided you with a primary collection notice covering the broader compliance workflow, including entity verification, PEP/sanctions screening, and risk scoring performed by other service providers, before your interaction with Scantek begins.

This Privacy Policy is for Users who are the subject of VOI and applies to personal information collected under scenarios 2, 3 and 4.

What personal information we collect and how we collect it

- Scantek collects your contact information from the Client or Platform who has requested your VOI, to initiate the VOI. All other personal information about you will be collected from you through the verification process with your consent.
- We collect your personal information as required to perform the VOI requested by the Client or Platform. This personal information will generally include full name, gender, date of birth, residential address, the type(s) of identification document(s) provided and their identification numbers. We may also receive your role in the relevant transaction or arrangement (for example, director, trustee, beneficiary, shareholder, or ultimate beneficial owner) and a transaction reference identifier linking your VOI to the compliance record maintained by the Client or Platform.
- We collect this information from Passports, both foreign and domestic, Australian Drivers Licences (or those issued under the laws of another country), Proof of Age Cards, Medicare Cards, Birth Certificates, and any other document presented or provided to Scantek by you.
- We collect images of the scanned and/or uploaded identification documents which will include any photographic image contained in the document.
- The image of any identification document provided by you may contain personal information not required for the VOI. Any information not required for the VOI is not recorded anywhere outside the image and is held only for as long as the image is required to be held.
- To verify your identity we must capture an image of you to compare with the images on identification documents you have provided. Your image is biometric information and therefore sensitive information under the Privacy Act and the Australian Privacy Principles and is treated accordingly. Sensitive information can only be collected when it is required for the purpose of verifying your identity and with your consent. Where Scantek's verification interface is accessed through a third-party Platform, the verification screen may be identified as "Powered by SCANTEK" within the Platform's interface and Scantek will separately obtain your consent to the collection of biometric data before the biometric capture process commences.

- During a remote VOI you will also be asked to perform a number of actions which are a necessary part of a liveness check (to lessen the risk posed by deep fakes and other deliberate attempts to fool the VOI). The information captured during this process includes biometric information, which will only be collected with your consent and only be held for as long as it is required to be held for the Client or our regulatory or verification requirements.
- We do not disclose, use or adopt government identifiers except where the use and disclosure of the identifier is necessary to perform the VOI requested by the Client.
- The VOI process is likely to require some of your document details to be verified by checking them against the Attorney-General's Department's DVS or issuing authority. The information returned from the DVS or issuing authority may include additional personal and sensitive information (unsolicited information). This and any other unsolicited personal information will not be recorded other than in the form it was received and will be deleted as soon as practical.
- Depending on the products or services being provided by our Client, other verification checks may be required from third-party suppliers and public sources, including but not limited to providers of criminal checks, law enforcement agencies, government and statutory authorities, banks and financial institutions, regulatory and licensing bodies, credit agencies and education providers. You will be notified if we will be performing these additional verification checks and we will obtain your consent if there is a possibility that unsolicited personal information may be provided to us in the process.

Our regulatory obligations require that we track and record, in some form, the multiple "journeys" through our platform, which requires cookies. Our use of cookies are discussed further below.

How we use your personal information

In broad terms, Scantek collects, uses and holds your personal information if we have a valid lawful reason to do so, and so that we can:

- Specifically:
 - Verify your identity as part, or all, of the service we provide to the Client or Platform who requested your VOI by sending the information you provide to the DVS Hub, administered by the Attorney-General's Department, and matching the information (an "Information Match Request") against official records held by the government agency responsible for issuing the identity document (**document issuer**), following which the DVS Hub will advise us of whether the information you provide matches official records; and/or

- Where Scantek's services are used by a Platform, return the VOI result to the Platform for incorporation into the Platform's compliance record for the relevant transaction; and/or
- For a specific purpose that you have given consent for us to process your personal information for
- In general:
 - Minimise risks and protect against fraud, misuse or loss of data and personal information, and to improve our services.
 - Comply with laws, obligations or provide assistance to regulatory, government and law enforcement authorities.

Scantek's use of the DVS may involve use of third party systems and services.

How will the Attorney-General's Department handle your personal information?

The DVS Hub facilitates information transfer between us and the document issuer. The DVS Hub itself does not retain any personal information and the Attorney-General's Department cannot view or edit any of the personal information transmitted through the DVS Hub.

The Attorney-General's Department engages a third-party provider as a managed service provider for the DVS, who is required to adhere to the APP requirements and security standards to ensure the use and disclosure of personal information is limited to explicitly defined purposes including:

- for the purposes of the contract with the department; and
- to comply with any request under section 95C of the Privacy Act.

The Attorney-General's Department is authorised to operate the DVS Hub for the purpose of verifying individual's identities under the IVS Act and in accordance with the IVS Rules.

For more information on how the Attorney-General's Department may handle your personal information, see the Attorney-General's Department's 'Privacy Statement – Identity Verification Services' at: <https://www.idmatch.gov.au/resources/privacy-statement-identity-verification-services>.

How will the document issuer handle your personal information?

Your personal information will be shared by the Attorney General's Department via the DVS Hub with the government agency that issued your identity document to verify it against their official records. These agencies already hold your personal information as part of their official records, in line with their own privacy policies and legal obligations.

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 5
--------------------	----------------	---------------------------	---------

Security and storage

Scantek implements a comprehensive array of physical, technical, organisational, and administrative security measures to protect the Personal Information we hold from unauthorised access, use, and disclosure. Scantek uses specific measures to protect personal information, such as data encryption, firewall protections, access control policies, and backup processes.

The servers used for storing Customer data, which may include Personal Information, are operated by Amazon Web Services and are located in Sydney, Australia. These data centres are certified to SOC 1, SOC 2, and ISO 270001 standards, ensuring robust security protocols. They feature continuous, round-the-clock security, automatic fire detection and suppression systems, redundant power supply systems, and strict controls for physical access.

Data held on our servers is inaccessible to anyone who has not entered into a contract with Scantek that includes confidentiality obligations. Data is encrypted both in transit (when being sent to and from our servers) and at rest (when stored). Specifically, 256-bit SSL/TLS encryption is employed to protect data in transit, while 256-bit AES encryption safeguards data at rest.

Scantek maintains stringent policies and management oversight of security, and we conduct mandatory staff security awareness training. While we strive to protect the security of the Personal Information we hold, it is important to be aware that no method of transmitting data over the internet or storing data is completely secure. Scantek has contractual protections, encryption, strict access controls, and due diligence checks to ensure all Australian and overseas recipients comply with Australian privacy standards.

We use digital certificates to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure in the following ways:

- Scantek's certificates are to be used for approved purposes only and are not permitted to be distributed beyond our secure network.
- All Scantek certificates are only installed on our secure infrastructure.
- All passwords used to access Scantek's digital certificates are stored securely and in accordance with our Password policy.

What happens if you don't consent to providing personal information?

Your VOI has been requested by a Client or Platform. If you do not wish to provide the requested personal information to Scantek for this purpose you should contact the Client or Platform to use an alternate method of VOI.

When we may share your information

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 6
--------------------	----------------	---------------------------	---------

- Scantek shares sufficient details of your personal information with the requesting Client or Platform to enable them to meet the legal or other obligation for which they requested the VOI. This information is provided to the Client via our secure portal or secure API call.
- We may share limited personal information with the requesting Client to identify you or your VOI so that we may respond to a Client's enquiry about your VOI.
- With your consent and in order to use the services you have agreed with the Client, we may be required to provide your information to governing bodies such as Anti-Money Laundering (AML), Australian Criminal Intelligence Commission (ACIC) or Visa Entitlement Verification Online system (VEVO).
- If compelled by law, we may disclose your information, including personal information:
 - In response to a subpoena or similar investigative demand, a court order, or a request for cooperation from a law enforcement or other government agency; to establish or exercise our legal rights; to defend against legal claims; or as otherwise required by law. In such cases, we may raise or waive any legal objection or right available to us.
 - When we believe disclosure is appropriate in connection with efforts to investigate, prevent, or take other action regarding illegal activity, suspected fraud or other wrongdoing; to protect and defend the rights, property or safety of our company, our users, our employees, or others; to maintain optimal operation of the system; to comply with applicable law or cooperate with law enforcement; or to enforce our terms and conditions or other agreements or policies.
- In the event of a reorganisation, merger, or sale of Scantek we may transfer any and all personal information we collect to the relevant third party.

Limited circumstances we may send personal information to overseas recipients

Scantek's own servers and data storage are hosted in Australia. Personal information collected by Scantek in connection with VOI is not routinely transferred to overseas recipients by Scantek. Generally Scantek keeps all personal information on third-party encrypted and secure servers within Australia.

There are three circumstances where personal information may be disclosed to or viewed by an overseas recipient:

- If the VOI being requested requires the verification of information by an overseas entity such as verification of a visa or other document not possible to verify through an Australian document verification service, this will only be done with your consent.

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 7
--------------------	----------------	---------------------------	---------

- In the unusual circumstance where the Client who has requested a VOI has staff involved in their processes who are working overseas. The Australian Document Verification Service only allows access to their services from within Australia except where an application for an exemption is made. These applications are made and approved by the DVS on a case-by-case basis.
- Where Scantek's services are accessed through a third-party Platform, that Platform may use additional service providers located overseas as part of its own compliance workflow (e.g. for PEP and sanctions screening or corporate registry lookups). Those overseas transfers are governed by the Platform's own privacy policy and are the Platform's responsibility under APP 8. Scantek does not control those transfers. You should refer to the Platform's privacy policy for details of any overseas processing within the broader compliance workflow.

Unsolicited personal information and de-identification

- We solicit and retain only personal information required to achieve accurate execution of our business activities and functions. Should we receive unsolicited personal information that information is destroyed immediately upon detection.
- We will de-identify personal information collected and stored where it is appropriate and practicable to do so.

Third Party Platforms

Scantek's identity verification services may be accessed through a Platform as part of an AML/CTF workflow solution acting on behalf of a reporting entity such as a conveyancer, financial services provider, accounting firm or law firm. In those circumstances the Platform will generally have provided you with a collection notice before any identity verification with Scantek begins. Scantek separately obtains your express consent to the collection of your biometric information directly through its verification interface (which may be presented as "Powered by SCANTEK" within the Platform's workflow) before that collection commences.

Where your VOI is initiated through a third-party Platform, queries about the broader compliance record held by the Platform should be directed to the Platform. Queries about the personal information and biometric data processed by Scantek specifically may be directed to Scantek using the contact details in this document. The Platform's own privacy policy governs how it handles your information in the context of any broad AML/CTF verification process.

The Attorney-General's Department's verification assistance service

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 8
--------------------	----------------	---------------------------	---------

There may be circumstances in which we will require assistance to verify your identity. If we request assistance from the Attorney-General's Department to verify your identity through the DVS, the Attorney-General's Department will collect your personal information for the purposes of verifying your identity document(s) through the DVS.

The Attorney-General's Department may also disclose your personal information to the relevant document issuer to assist them with verifying your identity documents. This collection is authorised under APP 5.2(c) and section 27 of the IVS Act and is conducted in accordance with the IVS Rules, which permits the collection of your personal information from someone other than yourself when it is authorised under an Australian law.

The Attorney-General's Department will handle your personal information in accordance with their obligations under the Privacy Act.

Where the identity document(s) you require to be verified include information regarding other individuals (such as a Medicare card covering multiple individuals), it will be assumed that you have advised those individuals and obtained their consent to the disclosure. This information will only be used for the purposes of verifying your identity document(s) through the DVS. Any personal information of other individuals will otherwise be managed in the same way as your personal information.

There may be overseas disclosure of your personal information to recipients located in New Zealand where New Zealand government agencies or private organisations request for verification assistance of your identity document(s).

If you don't provide your personal information to the Attorney-General's Department, the Department will be unable to verify your identity document(s).

More information about the verification assistance service is set out in the Attorney-General's Department's Identity Verification Services [Privacy Statement](#).

For more information about making complaints relating to the collection, use and disclosure of Identification Information for the purposes of requesting and provision of the DVS, see the section titled "*Complaints*" below.

You can find more information about the operation and management of the DVS Hub at <https://idmatch.gov.au>.

Integrity and retention of Personal Information

Scantek takes reasonable steps to ensure as far as possible that the personal information it collects is accurate and complete as at the date it was provided. VOI is transactional in nature and the personal information provided is not stored to be used in the future. We have no use for, or ability to, maintain up-to-date information.

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 9
--------------------	----------------	---------------------------	---------

We will retain your personal information for the period necessary to fulfil the purpose for which the personal information was provided, and no longer than is allowed by applicable law and regulations.

Where Scantek's VOI services are used in connection with a Platform, the Platform may be required to retain relevant records for a period of 7 years after the transaction is completed. That obligation rests with the relevant reporting entity utilising the Platform and is subject to the Platform's own data policies.

You are entitled to know and confirm the accuracy of all your personal information recorded by Scantek and all such requests will be addressed free of charge.

However, personal information from a VOI is held on behalf of the Client or Platform who requested the VOI and any requests in relation to this information must be directed to the Client or Platform. The Client or Platform will contact Scantek on your behalf, if necessary.

If for some reason such access is not granted, a written reason will be provided.

Request for Correction of Personal Information

Correction of personal information may not be possible once a VOI is completed as this information has been used to verify your identity. During the VOI you will be presented with the opportunity to correct any data our system has not properly recorded from your identity document. If the incorrect data is sent to the DVS or other issuing authority then the VOI may not complete, and the verification may be invalid (or not complete) and need to be resubmitted.

If we cannot correct personal information as requested, Scantek will respond in written form as to the reasons for denial of the correction along with the appropriate avenue for complaint. In this case should an individual request a statement be associated with that information, such a statement may be recorded and associated with the applicable data.

How long we keep your personal information

We aim to keep your information for only as long as we need it. Factors that may influence for how long we may keep your data include:

- Fulfilling our legal or regulatory obligations, and our Client's legal or regulatory obligations;
- Responding to a question or complaint; or
- Being unable to delete the data for technical reasons.

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 10
--------------------	----------------	---------------------------	----------

General Privacy Related Information

Collection and Use of Non-Personal Information

Scantek also collects data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

- We may collect information such as occupation, language, post code, area code, unique device identifier, location, IP location and the time zone where a Scantek product is used so that we can better understand customer behaviour and improve our products, services, and advertising.
- We may collect information regarding customer activities on our website, and from our products and services. This information is aggregated and used to help us provide more useful information to our customers and to understand which parts of our products, and services are of most interest. Aggregated data is considered non-personal information for the purposes of this Privacy Policy. If we combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.
- To provide location-based services on Scantek products, Scantek and our affiliates and licensees may collect, use, and share precise location data, including the real-time geographic location of the VOI.

Cookies and Other Technologies

Scantek's website, online services, interactive applications, email messages, and advertisements may use "cookies" and other technologies such as pixel tags and web beacons. These technologies help us better understand user behaviour, tell us which parts of our website people have visited, and facilitate and measure the effectiveness of advertisements and web searches. We treat information collected by cookies and other technologies as non-personal information. However, to the extent that Internet Protocol (IP) residential histories or similar identifiers are considered personal information by local law, we also treat these identifiers as personal information. Similarly, to the extent that non-personal information is combined with personal information, we treat the combined information as personal information for the purposes of this Privacy Policy.

We and our affiliates also use cookies and other technologies to remember personal information when you use our website, online services, and applications. Our goal in these cases is to make your experience with Scantek more convenient and personal.

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 11
--------------------	----------------	---------------------------	----------

Most browsers automatically accept cookies, but you can usually modify your browser setting to disable cookies. Please note that certain features of the Scantek website will not be available once cookies are disabled.

As is true of most websites, we gather some information automatically and store it in log files. This information includes Internet Protocol (IP) residential histories, browser type and language, Internet service provider (ISP), referring and exit pages, operating system, date/time stamp, and clickstream data.

We use this information to understand and analyse trends, to administer the site, to learn about user behaviour on the site, and to gather demographic information about our user base as a whole.

Pixel tags enable us to send email messages in a format customers can read, and they tell us whether mail has been opened. We may use this information to reduce or eliminate messages sent to customers.

We may use non-personalized information to monitor activity that deviates from the norm using Security Information and Event Management (SIEM) tools and takes appropriate action as part of our security and cyber crimes prevention processes.

Complaints

To exercise your rights under this Privacy Policy, or applicable law, or if you have a dispute regarding an individual's Personal information or the collection, use and disclosure of personal information for the purposes of requesting and provision of the DVS, you may do so by:

- Calling us on 1300 552 106
- or via the [Scantek website](#) contact page

We aim to respond to your dispute within 30 days. We take all complaints seriously and are committed to a quick and fair resolution. Individuals making complaints or enquiries will be afforded the right to anonymity where it is practicable to do so, however we may require certain information to confirm your identity.

If you are not satisfied with how we deal with your query or complaint, you may contact the Office of the Australian Information Commissioner (OAIC) by:

- calling their Privacy Hotline on 1300 363 992
- visiting the OAIC website.

For complaints specifically relating to the use of the Document Verification Service (DVS) and the collection, use and disclosure of Identification Information, you may find further

information about the DVS and how to make DVS-related complaints at:
<https://idmatch.gov.au>.

Children

Scantek does not knowingly collect personal information from children under 13. If we learn that we have collected the personal information of a child under 13 without first receiving verifiable parental consent we will take steps to delete the information as soon as possible.

Privacy Questions

If you have any questions or concerns about Scantek's Privacy Policy or data processing or if you would like to make a complaint about a possible breach of local privacy laws, please [contact us](#).

We may update our Privacy Policy from time to time. When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy

You may be asked to provide your personal information anytime you are in contact with Scantek or a Scantek affiliated company. Scantek and its affiliates may share this personal information with each other and use it, as long as the sharing and use are consistent with this Privacy Policy, the Privacy Act and the Australian Privacy Principles.

Our Company Wide Commitment to Your Privacy

Verification of Identity is Scantek's business, handling all personal information securely and in accordance with the Privacy Act is essential to that business.

Every new Scantek employee undertakes mandatory training in the identification and handling of personal information. Protection of personal information is discussed regularly in team and company-wide meetings, and considered when making any business decision.

Our Clients and relevant Platforms are contractually required to comply with the requirements of the Privacy Act, to comply with the privacy and other requirements of the Australian Document Verification Service (if applicable), the IVS Act and IVS Rules and to protect any personal information they receive. Our affiliates are required to apply the same privacy policies as Scantek, where applicable.

Document No: PO.06	Revision No: 1	Revision Date: 25/05/2026	Page: 13
--------------------	----------------	---------------------------	----------