Candidate Data Management Policy

Version	Date	Author	Description
1	July 2018	Tania Evans	Initial release of document.
2	Dec 2018	Tania Evans	Amended document references following external privacy and quality audit.
3	May 2019	Tania Evans	Amended document references following release of End User Licence Agreement.
4	June 2020	Tania Evans	Amended document references following annual review of Privacy Policy and End User Licence Agreement.
5	March 2021	Tania Evans	Amended document references following annual review of Privacy Policy.
6	October 2021	Ashliegh Fardon	Addition of definitions and information associated with WorkPro's Vaccination Status Management feature. Amended document references following review of Privacy Policy.
7	September 2022	Ashliegh Fardon	Amended document references following review of Privacy Policy. Updated terms in line with Candidate Terms of Access and omitted references to End User Licence Agreement (replaced with Client Terms of Access)
8	July 2023	Ashliegh Fardon	Updated to reflect deployment of Candidate Profile Deletion request and Data Retention policy

Policy Code	CDM03
Next Revision:	July 2024 unless otherwise required or dictated.
Approval Authority:	Chief Executive Officer, Chief Technology Officer, Chief Operations Officer

Purpose

Risk Solutions Australia Pty Ltd t/a WorkPro is committed to the appropriate storage of information in support of its operational, administrative and support functions. WorkPro acknowledges its obligation to ensure appropriate security of personal data as it relates to legislation while providing approved data storage solutions to accommodate the varying needs of WorkPro through the Licensed Services platform. The sensitivity of WorkPro Candidate Data is recognised and will be efficiently managed and availed through development of a best practice approach to Data Management.

This policy mandates a range of associated WorkPro policies, procedures and practices developed to ensure the integrity, authenticity, availability, access, confidentiality, security and destruction of

![WorkPro logo]

Candidate Data produced and/or utilised by WorkPro in addition to internal controls to mitigate identified risks.

Through its associated policies and procedures, WorkPro will:

- define the roles, responsibilities, and accountability for different data usage
- ensure best practice processes for effective Data Management including access, retrieval, reporting, managing, storing and destruction.

Legislation and Governance

- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- Information Privacy Act 2000 (Victoria)
- Electronic Transactions Act 2000 (Victoria)
- Australian Copyright Act of 1968
- Australian Crime Commission Act 2002 (Cth)
- Agreement for controlled access by duly accredited bodies to Nationally Coordinated Criminal History Checks (ACIC Agreement).
- Evidence Act 1958 (Victoria)
- Privacy Act 1988
- Australian Privacy Principles
- New Zealand's Information Privacy Principles, and
- the General Data Protection Regulation (EU) 2016/679 (GDPR).

Definitions

Term	Definition
ACIC	Refers to the Australian Criminal Intelligence Commission.
Candidate	A Workseeker who is registered to use the Licensed Services.
Customer	A WorkPro customer who is registered to use the Licensed Services to assist in meeting legal compliance obligations and to streamline engagement process for Candidates.
Data	All electronic data or information submitted by the Candidate making use of the Licensed Services, whether that data or information is submitted by the Candidate or data that is intended to be syndicated using the Licensed Services.
Data Management	Defines the access rights, roles and responsibilities in relation to the management and protection of the Data submitted in the Licensed Services platform.
De-identified	The process of removing Candidate profile information that would allow identification of the Candidate, including email address, mobile number, date of birth, residential address history, and postal address history. The Candidate will no longer have access to the De-identified profile within the Licensed Services.
Induction Verification	The number of induction/training certificates produced by the Customer which includes the learning/training modules and content that a Candidate has completed in WorkPro, including any customised module content. Induction verification does not refer to licences/ticket information viewed or residency status/visa check information validated through the integrated link with the Department of Home Affairs.
Licensed Services	Means the online, websites, web-based and mobile applications or platforms provided by WorkPro from time to time via a collection of

	software routines, protocols, functions, commands and tools which provide a User and Application Programming Interface that is accessible through a web browser and other designated platforms or websites from time to time to communicate with other third party software programs, operating in the same environment. The Licensed Services include, but are not limited to: a) any services that are arranged by you direct with WorkPro including administrative, monitoring, storage and monitoring services; and b) any associated offline and online Third Party Applications, browser hyperlinks, or components, including Application Programming Interfaces to Government bodies/entities and/or other third party providers that WorkPro has an agreement with to provide such services.
NPCS	Refers to the National Police Checking Service under contract to the ACIC.
Probity Check	Refers to the background checks available to be processed in the Licensed Services outside of a Police Check including but not limited to Credit Check, Bankruptcy Check, Employment History Check, Reference Check, Qualification Check.
Record	Any record that is created or received by WorkPro in the transaction of its business functions or resulting from Candidate activities and retained as evidence of that activity which can include, but is not limited to, hard copy documents, electronic or digital records including email and information maintained as part of using the Licensed Services.
Register	The act of registration as a user of the Licensed Services (including by means of Automated Access) and includes the act of registration on behalf of that person as a user, or the web-based confirmation of an act of acceptance of an invitation by any person to become a user.

Third Party Applications	Means online, web-based applications and offline software products that are:
	    a) provided by third parties;
	    b) interoperate with the Licensed Services; and
	    c) may be either separate or co-joined with the Licensed Services, whether or not they are identified to you by WorkPro as applications that are provided by third parties.

Vaccination Status Management	Refers to the WorkPro function that allows a Candidate to upload individual vaccination status, appointment dates and evidence including optional destruction of any Australian Government issued digital certificates once validated by the Customer as a vaccination digital certificate.
Vaccination Digital Certificate	The number of digital vaccination certificates produced by the Customer which includes the nominated vaccination status a Candidate has completed in WorkPro, that may include the Candidate's upload of an Australian Government issued digital certificate. Vaccination digital certificate does not refer to licences/ticket information viewed outside of WorkPro's Vaccination Status Management function.
Workseeker	Means a person who is or may be contemplating or seeking work in any capacity and includes a person who may already be in work and a person who may contemplating or seeking additional or alternative work.

Policy Statement

Principle	Demonstrated By

WorkPro will ensure the Candidate is informed about WorkPro's Data Management and privacy policies as they pertain to handling of Candidate data	• The Candidate is required to read and accept the terms of **WorkPro AU Privacy Policy** and **Candidate Terms of Access** when they Register in order to use the Licensed Services
Any candidate record generated as the result of WorkPro activities must be created, captured, stored, and effectively managed within WorkPro's approved data storage and records management systems	• Data collected by WorkPro is stored and encrypted within secure Microsoft Azure Data-centres as outlined in **WorkPro Data Security Statement**
Ownership and rights associated with data created, collected and stored is clarified and managed appropriately	• facilitating appropriate Data Management of all Data created or collected through the Licensed Services
The privacy context for the collection, management, storage and use of data is considered and addressed	• identifying data which is likely to pose legal issues to ensure storage and access options are suitably managed • ensuring that any privacy issues relevant to the collection, management and storage of data are addressed
Long term storage, archiving and disposal requirements are identified and implemented	• considering and implementing solutions for storing and accessing Data, as outlined in **WorkPro Data Security Statement** • retaining Data in compliance with minimum regulatory periods • disposing of Data in an appropriate manner in accordance with **NPCS Handbook**

Requirement to Retain Data for Compliance Purposes

As per **7. General Rights** of **Candidate Terms of Access**, there may be a requirement for Data to be retained for compliance purposes:

Outside of these compliance requirements, please refer to relevant Statute of Limitations in each jurisdiction:

- NSW
- ACT
- NT
- QLD
- SA
- TAS
- VIC
- WA

Specific Data Requirements

The below outlines WorkPro's default document retention periods. It is also applicable to profile deletion requests.

Induction and eLearning

Induction verification certificates remain valid for a maximum of 2 years (as determined by individual module expiry dates at the time of completion). After which time, any record of validation by a requesting Customer will remain within the Licensed Services in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in the remaining validation record are the module names that were validated, date of module completion, and any assessment results.

Citizenship and Work Rights

For a Non-Australian Citizen whose work rights have been validated using WorkPro's integration with the Department of Home Affairs Visa Entitlement Verification (VEVO) database:

- Document deletion occurs automatically 12 months after check completion
- Documents uploaded by the Candidate as part of the application and the result certificate returned from VEVO can be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function
- A report remains available through the Licensed Services and viewable by the requesting Customer as a record of verification in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in that record is the Candidate name, the time and date the check was processed, the outcome of the check the Visa expiry date, and a note of any document evidence provided.

For an Australian Citizen, whose citizenship has been validated using the Licenced Service:

- Document deletion occurs automatically 12 months after check completion
- Documents uploaded by the Candidate as part of the application can be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function
- The proof of verification remains available through the Licensed Services and viewable by the requesting Customer as a record of verification in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in that record is the Candidate name, the time and date the Citizenship was validated, and a note of the Citizenship evidence provided.

Australian Police Check

The data collected for the purpose of an Australian Police Check is stored, retained, and destroyed in adherence to ACIC guidelines outlined within the NPCS Handbook.

WorkPro Australian Police Check Conducted via NSS database

- Document deletion occurs automatically 12 months after check completion
- Results Certificate uploaded by the Candidate as part of the application can be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function
- Identity documents uploaded for the Police Check application and the Signed consent form must be retained for a minimum of 12 months, and no longer than 15 months

- The outcome remains available through the Licensed Services and viewable by the requesting Customer as a record of the check in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in that record is the Candidate name, the time and date the Result Certificate was returned, the Check Result (*only* DCO/NDCO) and the Role and the Workplace for which the check was completed.

Shared Certificate

- Document deletion occurs automatically 12 months after nominated check release date
- Results Certificate uploaded by the Candidate as part of the request can be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function
- The proof of verification remains available through the Licensed Services and viewable by the requesting Customer as a record of verification in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in that record is the Candidate name, the time and date the Result Certificate was validated, and the Role and Workplace of the Result certificate.

License Ticket and Document

- The Candidate can remove or make private any document they freely uploaded as part of using Licence Ticket and Document function of the Licensed Services.
- These documents can also be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function.
- The only available information remaining will be on any record of validation by a requesting Customer in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in the remaining validation record are the document names and expiry dates (where applicable) of documents that were validated.

Probity Checks

- Document deletion occurs automatically 12 months after check completion
- Results Certificate can be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function
- A record remains available through the Licensed Services and viewable by the requesting Customer as a record of verification in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in that record is the Candidate name, the time and date the check was processed, and the outcome of the check.

Vaccination Digital Certificate

- Documents uploaded by the Candidate as part of the application can be removed at the request of the Candidate at any time using the 'Delete WorkPro account' function
- The proof of verification remains available through the Licensed Services and viewable by the requesting Customer as a record of verification in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above. The information included in that record is the Candidate name, the time and date the vaccination status was validated, and a note of the evidence provided.

Third Party Applications

WorkPro does not accept responsibility for deletion of Candidate Data in Third Party Application providers.

Candidate Request to Delete Data

The Candidate has the right to request their information be deleted at any time using the 'Delete WorkPro account' function. The candidate will be made aware of any requirement for Data to be retained as outlined in this policy and will need to accept these terms to have any applicable Records permanently removed as per **7. General Rights** of **Candidate Terms of Access**.

Should there be a requirement to retain any information as outlined in this policy, the Candidate profile will instead be de-identified in consideration of the **Requirement to Retain Data for Compliance Purposes** noted above.

Where an account is de-identified, WorkPro internal staff will have visibility over the email address for use in Candidate support queries only. This information will not be visible to the Customer.

Supporting Documents

- WorkPro Data Security Statement
- WorkPro AU Privacy Policy
- NPCS Handbook
- WorkPro Candidate Terms of Access

Responsibility

- The Systems and Quality Manager is responsible for monitoring the implementation, outcomes and scheduled review of this policy and its accompanying procedure/s
- The Chief Executive Officer, Chief Technology Officer and Chief Operations Officer is responsible for maintaining the content of this policy
- The Systems and Quality Manager is responsible for the administration support for the maintenance of this policy as directed by the Chief Executive Officer, Chief Technology Officer and Chief Operations Officer