Record keeping and audit data

Background

The Document Verification Service (DVS) Business User Terms and Conditions (**the Terms and Conditions**) and DVS Commercial Service Access Policy (**the Access Policy)** provide guidance on what your organisation should do with the information it receives to submit a DVS match request and what to do with the result.

The Terms and Conditions note:

> *13. Your use of the DVS must at all times comply with all applicable laws, without limitation including all relevant Privacy Laws.*

The Access Policy notes that your information security practices must be:

> *consistent with requirements of Australian Privacy Principle 11 which mandates that Organisations take reasonable steps to protect personal information from misuse, interference, loss, and from unauthorised access, modification or disclosure.*

The DVS user community is a diverse array of businesses with different requirements and regulations. As such, the definition of what data is necessary to keep varies from User To User.

As User requirements for data retention are different, Users should seek independent legal advice to determine what data should be kept. This advice must take into account Users' legal requirements and the balance between storing unnecessary personal information whilst keeping enough information to support the User's decision making processes.

Decision-making on DVS record keeping

Unless regulations applicable to an organisation provide clear guidance, Users are mostly left with a risk-based decision on what personal information should be captured and retained.

For example, a User may have to decide between keeping and storing the details of the document provided in order to provide accountability on the decision making process or not retaining the details of the document to avoid the risk of a data breach or misuse.

Below is a summary of what information is kept by the DVS and the document issuers/official record holders that may assist Users in assessing their risks.

The DVS does not retain any personal information submitted in a match request. Rather, the DVS records key audit data on the origin and nature of the request, including:

- which organisation submitted the request
- a unique reference number to cross reference with the User
- a unique reference number to cross reference with the document issuer/record holder
- the type of document that was queried
- what the verification result was
- key timing events for each match request.

The document issuers/record holders have their own record keeping obligations but generally they will record:

- the unique reference code supplied by the DVS
- what record was queried
- if it succeeded/failed
- reason for a failure e.g. first name did not match
- key timing events for the match request.

The way data is collected will vary from User to User, however all Users should maintain basic information about the origin and purpose of each request. This might be linking the request to a customer record, recording IP addresses or other location information from a webform or a unique User ID where data entry is undertaken by employees of an organisation.

Privacy by design

The DVS has been built with privacy by design in mind.

The audit data that is kept by the User, the DVS and the document issuer/record holder has been specifically targeted so that information relating to the document can be obtained with a valid legislative basis whilst ensuring that each party involved does not store any unnecessary personal information.

The key to this is the unique reference numbers recorded in the DVS which link individual requests from the User to the document issuer/record holder. These numbers are stored in the DVS logs and can be used to link a transaction to the personal identity document on which verification was attempted if required for law enforcement purposes.

Use Case Example

- An individual completes an online form for a credit card and provides the User with a Victorian driver licence to confirm their identity.
- The User keeps location information from the individual who accessed the webform and the User's systems create a customer record that includes the person's preferred name, email address and mobile phone number but the User does not keep the person's date of birth or driver licence type/number.
- Subsequently, it is discovered that the credit card was not issued to the true holder of the identity document (identify takeover) and a valid law enforcement investigation commences. The User did not keep the details of the Victorian driver licence submitted.
- Law enforcement contacts the User who provides the reference number to provide o Home Affairs.
- Law enforcement contacts Home Affairs who can provide the corresponding request number and the details of the transaction.
- Law enforcement then contacts the document issuer to get the personal identity information.

Conclusion

- Home Affairs mandates Users collect audit data about the origin and unique nature of each match request as well as the unique reference number provided to the DVS.
- Users should seek their own legal advice regarding what additional personal detail is retained and for how long.
- Consideration should be given to the DVS' design to review if key personal information can be recovered via other methods without the User needing to store personal information about the document verified.