Australian Government
Department of Home Affairs

DVS DOCUMENT VERIFICATION SERVICE

DOCUMENT VERIFICATION SERVICE (DVS) COMMERCIAL SERVICE:

ACCESS POLICY

VERSION 4

A. Purpose

This Document Verification Service (DVS) Commercial Service Access Policy ('the Policy') outlines the criteria that private sector organisations ('Organisations') must meet in order to be eligible to access the DVS commercial service.

B. Background

The DVS is a secure online system that enables Organisations to confirm that information presented on identity documents matches that held by the document issuing agency. This can assist Organisations to make identity based decisions by providing greater assurance that the information presented on identity documents is legitimate.

The DVS can also help prevent the use of stolen or fraudulent identity documents, which in turn helps to prevent identity crime, protect privacy and promote greater confidence in the identities that Australians use to access a wide range of government and other commercial services.

As a key element of the *National Identity Security Strategy*, agreed by the Council of Australian Governments, the DVS is owned and operated by the nine governments of Australia. This responsibility is exercised by all jurisdictions through the National Identity Security Coordination Group and its supporting DVS Advisory Board (also referred to as DVS Agencies). Following the agreement of all Australian governments to provide DVS access to private sector organisations, a DVS Commercial Service commenced operation in early 2014.

Consistent with the objectives of all Australian governments to reduce regulatory impacts on industry, DVS Agencies will draw on existing regulatory and licensing regimes to help determine Organisations' eligibility for DVS access.

The DVS supports the rights and protections afforded to individuals under the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988.* In order to confirm the accuracy of information presented on documents commonly used as evidence of identity, DVS verifications involve the use of government identifiers. Organisations seeking to use the DVS therefore need to meet the requirements for the use of government identifiers that are outlined in the APPs.

C. Access Criteria

Private sector organisations applying to become DVS Business Users will need to meet the following access criteria.

1. ***Subject to the Privacy Act:*** The Organisation is subject to the *Privacy Act 1988 (Cth)* or the *Privacy Act 1993 (New Zealand).*

2. ***Based in Australia or New Zealand*:** The Organisation has a physical presence in Australia or New Zealand and is subject to local civil and criminal laws.

3. ***Permitted to use or disclose Government Related Identifiers:*** The Organisation can satisfy the requirements of APP 9.2 relating to the use or disclosure of government related identifiers, including one or more of the following:

    a. the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

    b. the use or disclosure of the identifier is reasonably necessary for the Organisation to fulfil its obligations to an agency or a State or Territory authority

    c. the use or disclosure of the identifier is reasonably necessary for the Organisation to verify the identity of the individual for the purposes of the Organisation's functions or activities; or

    Or if the Organisation is based in New Zealand, it can satisfy an equivalent requirement.

4. ***Regulated Entities:*** The Organisation is registered or licensed or operates under a regulatory regime operated by the Commonwealth, State and Territory or New Zealand Governments. This includes, but is not limited to:

    a. Commonwealth licencing schemes under the *Corporations Act 2001*, the *Banking Act 1959* and the *Telecommunications Act 1996*;

    b. State and Territory legislation relating to electronic conveyancing or electricity distribution or other legislation; or

    c. any equivalent New Zealand legislation.

5. ***Use of Gateway Service Provider:*** The Organisation accesses the DVS through an approved Gateway Service Provider (GSP) or successfully applies to become a GSP in its own right.

6. ***Requirements for DVS Use:*** The Organisation has the capacity and agrees to comply with all requirements for use of the DVS commercial service, including but not limited to:

   a. obtaining the informed consent of its clients for DVS matching

   b. only using the DVS for the purpose(s) for which access has been granted

   c. information security and access controls, including logging and monitoring use of the system

   d. compliance reporting, and

   e. being reasonably subject to independent audits of its use of the DVS.

   ID Service Provider specific requirements:

   f. ensuring IDSP clients meet the DVS Access Criteria

   g. ensuring that a comprehensive list of IDSP clients is provided to the nominated GSP and is kept up to date, and

   h. ensuring that all disclaimers, exclusions, limitations of liability and indemnities that form part of the contractual arrangements with is ID Service clients are also for our (the DVS Manager's) benefit and can be directly enforced by the DVS Manager.

D. Using or disclosing Government related identifiers

In accordance with the Privacy Act 1988, the primary responsibility for assessing and demonstrating that an Organisation may use or disclose government related identifiers (i.e. to use the DVS) rests with the Organisation itself.

Prospective DVS Business Users may wish to refer to the supporting guidelines to this policy for further information on assessing reasonable necessity.

E. Consideration of applications

Applications for access to the DVS Commercial Service will be considered by DVS Agencies, which are not under any obligation to provide an individual Organisation with access to the DVS.

However, in most cases DVS Agencies will approve applications from prospective DVS Business Users where:

   a. the Organisation meets the criteria outlined in this policy;

b. the Organisation pays the applicable fees at the time of application; and

c. DVS Agencies do not have a specific and material objection to the Organisation being provided with access to the DVS.

Australian Government
Attorney-General's Department

DVS DOCUMENT VERIFICATION SERVICE

DOCUMENT VERIFICATION SERVICE (DVS) COMMERCIAL SERVICE:

ACCESS GUIDELINES

VERSION 3

Table of Contents

F. Purpose

These *Document Verification Service (DVS) Commercial Service Access Guidelines* ('the Guidelines') are designed to provide further *information* on the criteria that private sector organisations ('Organisations') must meet in order to be eligible to access the DVS commercial service, as outlined in the *DVS Commercial Service Access Policy* ('the DVS Access Policy').

The Guidelines are intended to assist:

- Organisations in completing applications for DVS Business User access;
- DVS Agencies in assessing applications for DVS Business User access; and
- Both DVS Business Users and DVS Agencies in ensuring that terms and conditions of DVS access continue to be met while an Organisation uses the system.

These Guidelines draw upon the *Australian Privacy Principles Guidelines* (the APP Guidelines) produced by the Office of the Australian Information Commissioner. They should be read in conjunction with the APP Guidelines, the DVS Access Policy, and the terms and conditions applicable to DVS Business Users.

These Guidelines do not represent a legal opinion on the requirements of the *Privacy Act 1988*. Organisations that are concerned about their privacy obligations should seek independent legal advice.

G. DVS Access Policy Criteria

The DVS Access Policy outlines a number of criteria and Organisations must satisfy all of these criteria in order to be provided with DVS access. These criteria can be summarised as follows:

Access Criterion 1: Subject to the Privacy Act

Access Criterion 2: Based in Australia or New Zealand

Access Criterion 3: Permitted to Use or Disclose Government Related Identifiers

Access Criterion 4: Regulated Entities

Access Criterion 5: Use of Gateway Service Provider

Access Criterion 6: Requirements for Use of the DVS

Further information on these criteria and their application is contained in the following sections of these Guidelines.

H. Access Criterion 1: Subject to the Privacy Act

H.1. Subject to the Privacy Act: The Organisation is subject to the Privacy Act 1988 (Cth) or the Privacy Act 1993 (New Zealand).

H.2. The Privacy Act 1988 (Cth) (the Australian Privacy Act)

The Privacy Act 1988 (Cth) contains the Australian Privacy Principles (APPs), which outline responsibilities for the collection, use, storage and disclosure of personal information. Organisations that are subject to these and other Privacy Act requirements are known as 'APP entities'. They include Organisations that may not normally be covered by the Act, but which choose to 'opt-in' by formally registering with the Privacy Commissioner.

Organisations automatically subject to the Australian Privacy Act

In general terms, an Organisation will be *automatically* bound by the Australian Privacy Act if it has an annual turnover of more than $3 million in a financial year.

Organisations otherwise subject to the Australian Privacy Act

Businesses with a yearly turnover of $3 million or less may also be subject to the Australian Privacy Act if they:[1]

- provide a health service and hold health information other than in an employee record, or
- collect or disclose another person's personal information as part of their business to provide a benefit, service or advantage (unless they do so with that person's consent or as authorised by law), or
- are a contracted service provider with a Commonwealth contract, or
- are a reporting entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

Opting-in to the Australian Privacy Act

Other businesses with a yearly turnover of $3 million or less may formally register with the Privacy Commissioner to 'opt in' to be subject to the Australian Privacy Act.

A business can opt-in by filling in the designated application form and being placed on the public Opt-in Register by the Privacy Commissioner. More information on opting-in can be found on the website of the Office of the Australian Information Commissioner.

[1] Adapted from the Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines* (Privacy Act 1988) February 2014 (the APP Guidelines), B.3-7.

H.3. The Privacy Act 1993 (New Zealand) (the New Zealand Privacy Act)

DVS access may also be provided to businesses in New Zealand, as all these organisations are subject to the New Zealand Privacy Act.

This Act binds any 'agency', which is defined broadly to mean 'any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector'.[2]

The New Zealand Privacy Act contains a range of protections over the use of personal information.

I. Access Criterion 2: Based in Australia or New Zealand

Based in Australia or New Zealand: The Organisation has a physical presence in Australia or New Zealand and is subject to local civil and criminal laws

DVS access may only be provided to Organisations that are either based in Australian or New Zealand. This includes Organisations that have a physical presence in either country, even though the parent company may be based overseas.

This requirement helps to ensure that, in the event that an Organisation misuses the result of a DVS check, the Organisation may be subject to civil or criminal proceedings under Australian or New Zealand law, as appropriate. This includes the ability for the affected individual(s) to seek redress from the Organisation under civil law.

For the purposes of DVS access, an Organisation is considered to be based in Australia or New Zealand where it is:[3]

- an Australian or New Zealand citizen or permanent resident, or
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law, or
- a partnership formed, or a trust created, in Australia, an external Australian Territory, or New Zealand, or
- a body corporate incorporated in Australia or New Zealand, or
- an unincorporated association that has its central management and control in Australia, an external Australian Territory or New Zealand.

[2] *The Privacy Act 1993 (New Zealand)*, s 2.
[3] Adapted from the *Privacy Act 1988 (Cth)* s 5B(2), APP Guidelines, B.10 – B.12

This is an additional requirement to that in Criterion 1, as an Organisation may be subject to Australian privacy law (i.e. have an 'Australian Link'_) without necessarily being based in Australia.

J. Access Criterion 3: Permitted to use or disclose Government Related Identifiers

Permitted to Use or Disclose Government Related Identifiers: The Organisation can satisfy the requirements of Australian Privacy Principle 9.2 relating to the use or disclosure of government related identifiers, by one or more of the following:

a. the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

b. the use or disclosure of the identifier is reasonably necessary for the Organisation to fulfil its obligations to an agency or a State or Territory authority; or

c. the use or disclosure of the identifier is reasonably necessary for the Organisation to verify the identity of the individual for the purposes of the Organisation's functions or activities.

Or if the Organisation is based in New Zealand, it can satisfy an equivalent requirement.

J.1. Australian Organisations

DVS verifications involve the handling of government related identifiers, such as document numbers on passports, driver licences, and Medicare cards.

The Australian Privacy Act restricts the adoption, use and disclosure of government related identifiers by private sector organisations, unless the organisation can meet one of the specified exceptions. These exceptions to the use and disclosure of government related identifiers are outlined in Australian Privacy Principle 9.2 and include that the use or disclosure of the identifier is:[4]

- required or authorised by or under an Australian law or a court/tribunal order.[5]
    - This exception relates to both Commonwealth and State and territory legislation.

[4] Adapted from APP Guidelines, 9.22-9.30.
[5] Australian Privacy Principle 9.2(c)

- reasonably necessary for the Organisation to fulfil its obligations to an agency or a State or Territory authority.[6]
    - This exception, which includes non-legislative obligations, is most likely to be relevant to a contracted service provider, and will allow them to use or disclose a government related identifier if this is reasonably necessary to perform a Commonwealth or State or Territory contract.
- reasonably necessary for the Organisation to verify the identity of the individual for the purposes of the Organisation's functions or activities.[7]
    - This exception allows an Organisation to use a government related identifier both to establish the identity of an individual and to verify that an individual is who or what they claim to be, for example, to verify their name or age.

J.2. New Zealand Organisations

For the purpose of DVS access, corresponding access criteria have also been developed for New Zealand Organisations that are subject to the New Zealand Privacy Act. These allow DVS access to be granted to Organisations, where the use or disclosure of an Australian government related identifier is:

- required or authorised by or under a New Zealand law or a court/tribunal order; or
- reasonably necessary for the Organisation to fulfil its obligations to New Zealand Government authority; or
- reasonably necessary for the Organisation to verify the identity of the individual for the purposes of the Organisation's functions or activities; and
- consistent with any relevant Australian law or regulations.

J.3. Identifying the functions and activities of an Organisation

In the context of the Australian Privacy Act, an Organisation's functions and activities include:[8]

- the current functions or activities of the Organisation,
- proposed functions or activities that the Organisation has decided to carry out and for which it has established plans; and

[6] Australian Privacy Principle 9.2(b)
[7] Australian Privacy Principle 9.2(a)
[8] APP Guidelines, 3.13.

- activities that the Organisation carries out in support of its other functions and activities, such as human resources, corporate administration, property management and public relations activities.

The functions and activities of an Organisation will commonly be described (though not necessarily exhaustively) on a website, in an annual report, and in corporate brochures, advertising, product disclosure statements and in client and customer letters and emails.[9]

The functions and activities of an Organisation (for which it may collect and use personal information under the Privacy Act) are limited to those in which it may lawfully engage.[10]

J.4. Determining Reasonable Necessity

It is the responsibility of a prospective DVS Business User, as an APP entity, to be able to justify that the use and any disclosure of a government related identifier (i.e. as the result of using the DVS) is in accordance with the exceptions provided in Australian Privacy Principle 9.2.[11]

The exception in APP 9.2(a) allows an Organisation to use or disclose a government related identifier where it is reasonably necessary for the Organisation to verify the identity of the individual for the purposes of the Organisation's functions and activities. The exception in APP 9.2(b) allows an Organisation to use or disclose a government related identifier where it is reasonably necessary to fulfil its obligations to an agency or a State or Territory authority.

The 'reasonably necessary' test is an objective test: it is a question of whether a reasonable person who is properly informed would agree that the use or disclosure is necessary (not merely from the perspective of the Organisation proposing to undertake the activity). The test must be applied in a practical sense.[12]

In general terms, if an Organisation cannot, in practice, effectively pursue a lawful function or activity without using or disclosing a government related identifier in order to verify a person's identity, the use of the identifier would usually be considered reasonably necessary for that function or activity.

Where an Organisation is seeking to determine whether it has a reasonable necessity to use and disclose a government related identifier to verify a person's identity for the

[9] APP Guidelines, 3.14.
[10] Adapted from APP Guidelines, 3.15.
[11] Adapted from APP Guidelines, B.108.
[12] Adapted from the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Explanatory Memorandum; APP Guidelines, B.108/9.

purpose of the Organisation's functions or activities, such as by using the DVS, it may be relevant to consider whether the use or disclosure of the government related identifier:

- ensures the Organisation is not unreasonably exposed to risks resulting from identity crime or other serious crime, having regard to the entity's functions or activities
- provides a more privacy-enhancing means of identity verification than alternative methods.

These examples are provided for illustrative purposes only to assist Organisations in interpreting the requirements of APP 9.2(a).

It may not be reasonably necessary to use or disclose a government related identifier to verify the identity of an individual or fulfil its obligations to an agency or State or Territory authority where there are reasonable alternatives available. This includes situations where:[13]

- the Organisation can carry out the function or activity, or fulfil its obligations to an agency or State or Territory authority, without verifying the individual's identity, for example:
    - where de-identified information would be sufficient for the function or activity; or
    - where a deposit or other financial guarantee would be sufficient for the function or activity
- there are other practicable means of verifying the individual's identity available to the Organisation, for example:
    - by using or disclosing other types of personal information, rather than the government related identifier; or
- the Organisation has an established history of transacting with the individual.

In this context, Organisations should note their obligation to provide individuals with an option to transact on the basis of pseudonymity or anonymity, where this is not impracticable for the Organisation to do so.[14]

There are also other exceptions in APP 9.2 that allow an Organisation to use or disclose a government related identifier. These include where the use or disclosure is:

- required or authorised by or under an Australian law or a court/tribunal order

[13] APP Guidelines, 9.28.
[14] Australian Privacy Principle 2.

- necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health, and it is unreasonable or impracticable to gain the consent of the individual; or
- necessary for the entity to take appropriate action in relation to suspected unlawful activity or serious misconduct that relates to the entity's functions or activities.

J.5. Incorrectly Claiming the Organisation is permitted to use or disclose a government related identifier

Should an Organisation incorrectly claim to be able to use or disclose a government related identifier under an exception in APP 9.2 (for example, by incorrectly claiming it has a reasonable necessity to use the government related identifier to verify the identity of the individual for the purposes of the Organisation's functions or activities) , and subsequently use or disclose the identifier, including as a result of using the DVS, this may constitute a breach of Australian Privacy Principle 9.2 and therefore constitute 'an interference with the privacy' of an individual.

The Privacy Commissioner can investigate possible interferences with privacy, either following a complaint by the individual(s) concerned or on the Commissioner's own initiative. The Commissioner has a range of enforcement powers and other remedies available.

J.6. Illustrative Examples of Reasonable Necessity

Some indicative examples or purposes for which Organisations may be either more likely or unlikely to be able establish a reasonable necessity to use or disclose a government related identifier to verify the identity of an individual for the purposes of the Organisation's functions or activities, or to fulfil its obligations to an agency or a State or Territory authority, are provided at **Attachment A**.

K. Access Criterion 4: Regulated Entities

Regulated Entities: The Organisation is registered or licensed or operates under a regulatory regime operated by the Commonwealth, State and Territory or New Zealand Governments. This includes, but is not limited to:

a. Commonwealth licencing schemes under the Corporations Act 2001 (Cth), the Banking Act 1959 (Cth) and the Telecommunications Act 1996 (Cth); Anti-Money Laundering and Counter-Terrorism Financing Act 2006; or

b. State and Territory legislation relating to electronic conveyancing, or electricity distribution, or other Act or regulations; or
c. any equivalent New Zealand legislation.

Organisations that are not subject to a relevant regulatory or licensing regime will be considered on a case by case basis.

The fact that an Organisation is registered, licenced or otherwise operates under a recognised regulatory regime can provide additional confidence that an Organisation has a reasonable necessity to use or disclose government related identifiers. For example, existing licensing helps to establish that the purpose for which the Organisation is seeking DVS access is a legitimate function or activity for that type of entity, and that the Organisation and its principals are of good standing.

This can also provide DVS Agencies with additional confidence that an Organisation is subject to existing compliance activities (e.g. inspections) which can be taken into account in the application of the DVS audit and compliance regime.

In applying for DVS access, Organisations must nominate existing registration, licensing or regulatory regimes, including legislative and non-legislative schemes, to which they are subject. A list of relevant regimes is available on the DVS Website.

L. Access Criterion 5: Use of Gateway Service Provider

Use of Gateway Service: The Organisation accesses the DVS through an approved Gateway Service Provider (GSPs) or successfully applies to become a GSP in its own right.

The DVS utilises GSPs as commercial intermediaries to connect DVS business users to the system. This approach helps to minimise upfront connection and ongoing transaction costs for business users, consolidate physical connections to the DVS Hub and associated security and access management controls, and to offer a market-based solution to encouraging DVS use.

GSPs also play an important role in DVS risk management and compliance arrangements. As the entities dealing directly with DVS business users, on an ongoing basis, GSPs are well placed to identify any potential misuse of the system. For this reason, GSPs are responsible for entering into contracts with DVS Users on behalf of DVS Agencies. These contracts contain the terms and conditions of DVS access that an Organisation must continue to meet throughout its use of the system.

Details on applying for the DVS through a GSP are provided on the DVS Website.

Organisations interested in becoming GSP should contact DVS.Manager@ag.gov.au.

M. Access Criterion 6: Requirements for Use of the DVS

Requirements for Use of the DVS: The Organisation has the capacity and agrees to comply with all requirements for use of the DVS commercial service, including but not limited to:

a. obtaining the informed consent of its clients with regard to DVS matching
b. only using the DVS for the purpose(s) for which access has been granted
c. information security and access controls, including logging and monitoring use of the system
d. compliance reporting, and
e. being reasonably subject to independent audits of its use of the DVS.

ID Service Provider specific requirements

f. ensuring IDSP clients meet the DVS Access Criteria
g. ensuring that a comprehensive list of IDSP clients is provided to the nominated GSP and is kept up to date, and
h. ensuring that all disclaimers, exclusions, limitations of liability and indemnities that form part of the contractual arrangements with its ID Service clients are also for our (the DVS Manager's) benefit and can be directly enforced by the DVS Manager.

The DVS is only offered to organisations that have the capacity and agree to comply with the requirements of DVS use. These are detailed in the terms and conditions which are provided on the DVS Website, and which are included in business user contracts.

M.1. DVS Access Terms and Conditions

As outlined below, these requirements reflect the best practice privacy and security arrangements that are expected of all DVS Users:

a. *Consent* – Obtaining express consent for DVS matches reflects best practice when interacting with individuals.
   - Consent means 'express consent or implied consent'.[15]
   - According to the APP Guidelines, consent has four key elements:[16]

[15] *Privacy Act 1988 (Cth), s 6(1)*
[16] APP Guidelines, B.29.

i. the individual is adequately informed before giving consent
ii. the individual gives consent voluntarily
iii. the consent is current and specific, and
iv. the individual has the capacity to understand and communicate their consent.

Depending on their business processes, Business Users may need to include a written explanation of how their customers' personal information will be used in order to gain their informed consent. For example:

> *The document details you provided as evidence of your identity will be checked with the relevant government agency via the Document Verification Service. You can find more information about the Document Verification Service at [insert Website] or by telephoning/writing to [insert telephone number, fax number or post office box number]*

Business Users may also include an explanation of the consequences of *not* providing consent, for example:

> *If you do not provide your driver licence or passport number or your document is not verified by the Document Verification Service, we may not be satisfied as to your identity and you may not be able to open an account with us online.*

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent. [17]

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves. [18]

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.[19]

Business users should consult the APP Guidelines for further information on consent.

[17] APP Guidelines, B.56.
[18] APP Guidelines B.57.
[19] APP Guidelines, B.58.

b. *Appropriate use* – Use of the DVS for a purpose other than that for which access was granted may constitute an unauthorised use of government related identifiers – i.e. a breach of Australian Privacy Principle 9.2.
    - An unauthorised secondary use might occur, for example, where an Organisation which has been granted DVS access as is 'reasonably necessary' for pre-employment screening, subsequently uses the service to support a customer loyalty program.

c. *Information security* – Security measures such as access controls, including logging and monitoring use of the system, represent industry best practice.
    - They are also 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.

Other terms and conditions help ensure that any potential privacy or other risks associated with DVS use can be identified and managed effectively:

d. *Compliance reporting* – This is an essential part of the DVS risk management regime that is designed to prevent unauthorised use of the system
    - Compliance reporting is an essential part of the DVS's risk and compliance regime.

e. *Independent audits* – As another key part of the DVS risk management regime, DVS Users must agree to be subject to independent audits of their use of the system.
    - Where an Organisation's operations cannot be audited without an unreasonable financial, resource or other burden on DVS Agencies, the Organisation may either:
        i. Be asked to contribute to the cost of any independent audits; or
        ii. Have an application for DVS access declined, or any existing DVS access terminated.

M.2. Compliance with DVS Access Terms and Conditions

GSPs and the Attorney-General's Department actively monitor the use of the DVS, including through transaction monitoring, targeted auditing and spot checks. Non-compliance with DVS terms and conditions will constitute a breach of contract.

A breach of terms and conditions may result in legal action being taken by the relevant GSP or the Attorney-General's Department, without further recourse to the Organisation.

In more serious cases, misuse of the DVS may also involve offences under the Commonwealth and/or State and Territory criminal codes. Where any criminal conduct involving use of the DVS is suspected, the matter will be referred to the relevant law enforcement agencies.

A suspected or actual breach of privacy law can result in the suspension or termination of DVS access.

N. Application Process

N.1. Consideration of applications

Only complete applications will be considered. Any information or documentation that is missing from an application may delay its consideration and/or approval.

The application process is detailed on the DVS Website, and may be subject to revision, but will include the following elements:

Application

Business user applications need to include the following elements:

- Evidence of the Organisation being subject to Privacy Act, including the Organisation's privacy policy
- Details of relevant regulatory regime(s)
- Purpose(s) for seeking DVS Access, including:
- details of legislative authorisation to use government related identifiers, or
- a declaration of 'reasonable necessity' to use government related identifiers
- Volume estimates,
- Authority to enter into a contract.

Evidence of prior agreement

Applicants should also nominate a GSP(s), although applications will be accepted pending notification of the selected GSP(s).

Review of Applications (Due diligence)

Appropriate checks will be conducted with relevant regulators, including ASIC, ACMA, and the OAIC, to confirm the accuracy of information provided as part of the application process and to ensure the Organisation and its principals are of good standing.

N.2. Specific and material objections

The DVS Access Policy indicates that DVS Agencies (or other delegated decision-makers) will approve applications that meet the DVS Access Criteria, and are

accompanied by the applicable application fees, unless DVS Agencies have a specific and material objection to the Organisation being provided with access to the DVS.

Any concerns raised by DVS Agencies (or other delegated decision-makers) over the suitability of an Organisation applying for DVS access will be dealt with on a case-by-case basis.

Without seeking to prescribe or limit the factors that may constitute a 'specific and material objection' to providing an Organisation with DVS access, these may include cases where:

- the Organisation has been responsible for breaches of the Privacy Act that have not been resolved to the satisfaction of the Privacy Commissioner;
- information is made available to DVS Agencies (or other delegated decision-makers) that suggests that an Organisation may be involved in unlawful activities; and
- information is made available to DVS Agencies (or other delegated decision-makers) that suggests that one or more persons involved in the management or operations of the Organisation may not be a 'fit and proper person'.

O. Further information

Further information about DVS access, including contact details for the DVS management and Gateway Service Providers, as well as business user terms and conditions, are available on the DVS website.

Questions on privacy obligations should be referred to the relevant privacy regulator, in Australia or New Zealand.

P. Attachment A – Reasonable necessity and the DVS: Illustrative Examples

The following examples are designed to illustrate the purposes for which an Organisation may have a reasonable necessity to use or disclose government related identifiers to verify a person's identity, or to fulfil its obligations to an agency or a State or Territory authority, and accordingly to use the DVS. In some of these cases, an Organisation's use or disclosure of the identifier may also be required or authorised by or under an Australian law.

These examples are provided for illustrative purposes only to assist Organisations in interpreting the requirements of APP 9.2.

Australian Privacy Principle 9.2(a): reasonably necessary to verify the identity of the individual for the purpose of the Organisation's activities or functions

Some examples of purposes for which an Organisation may be more likely to be able to establish a reasonable necessity to use or disclose government related identifiers to verify the identity of an individual, with a person's express consent (i.e. use the DVS) for the purposes of the activities or functions of the Organisation include:

- pre-employment screening
- enrolling students in educational institutions
- providing evidence of parent/guardian status when acting on behalf of a child
- property rentals
- property purchases (conveyancing)
- motor vehicle hire
- hire of plant, machinery or other equipment
- provision of essential utilities such as energy, water or telecommunications services
- protecting children or other vulnerable persons from criminal or other inappropriate conduct, including online conduct
- entering into a binding legal contract involving significant financial or other liabilities.

Some examples of purposes for which an Organisation may be *unlikely* to be able to establish a reasonable necessity to use or disclose government related identifiers to verify the identity of an individual, even with a person's express consent (i.e. use the DVS), for the purposes of the activities or functions of the Organisation include:

- customer loyalty programs
- registering with a social network
- booking or registering to stay in hired accommodation
- purchasing lower value goods or services (i.e. purchases for which identity verification would not be required were the transaction to be conducted in person, or where a deposit would be practicable to mitigate financial risk).

Australian Privacy Principle 9.2(b): reasonably necessary for an Organisation to fulfil its obligations to a Commonwealth agency or a State or Territory authority

Some examples of purposes for which an Organisation may be more likely to be able to establish a reasonable necessity to use the DVS to fulfil its obligations, including non-legislative obligations, to a Commonwealth agency or a State or Territory authority include:

- Lodging documents with a government entity on behalf of a customer who needs to verify their identity (e.g. with ATO)

- Providing services on behalf of a government agency which involve the identification of individuals (e.g. employment assistance services, security screening)
- Compliance with a government-sponsored, non-legislated industry code involving identity verification (e.g. to restrict suspicious sales of hazardous chemicals).

Some examples of purposes for which an Organisation may be *unlikely* to be able to establish a reasonable necessity to fulfil its obligations, including non-legislative obligations, to a Commonwealth agency or a State or Territory authority include:

- Satisfaction of contractual obligations to a government agency which do not require identification of individuals (e.g. processing of payments or general recruitment without specific contractual requirements)
- Applying for a government grant
- Making an inquiry about an entitlement.