CLAYTON UTZ

Document Verification Service

National Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS

31 March 2015

Clayton Utz
Lawyers
Level 10, NewActon Nishi
2 Phillip Law Street
Canberra ACT 2601
GPO Box 9806
Canberra ACT 2601
Tel +61 2 6279 4000
Fax +61 2 6279 4099
www.claytonutz.com

Our reference 213/15921/80151527

Contents

1. Introduction and outline

The Document Verification Service (or in this document, the **DVS**) is a secure online system that enables organisations to verify information on documents issued by Australian Government and state and territory government agencies (in this document, **evidence of identity documents**) as against the records of the document issuing agency. The evidence of identity documents include immigration documents, passports, driver licenses, Medicare cards and birth certificates.

The DVS is currently available to government agencies and is being made available to private sector organisations that have Commonwealth legislative obligations to identify their customers (such as under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)).

DVS transactions currently involve a check of whether the information presented on an evidence of identity document matches the records of the issuing agency. The results are currently provided in the form of a 'yes/no' result.

The reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**) with effect from 12 March 2014 include amendments to the use by organisations of government related identifiers (previously dealt with by National Privacy Principle (**NPP**) 7.2). The key difference between NPP 7.2 and the new Australian Privacy Principle (**APP**) 9.2 is that the latter allows use of government related identifiers by organisations in different circumstances, including where "*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 activities or functions*." A government related identifier is defined as follows:

- government related identifier of an individual means an identifier of the individual that has been assigned by:

  (a) an agency; or

  (b) a State or Territory authority; or

  (c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or

  (d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

The current DVS access management policy limits commercial access and use to businesses operating under legislated client identification requirements. This restriction was informed by the prohibitions and permissions of the Privacy Act (NPPs 7.2, 2.1). In the light of the privacy reforms the Commonwealth Attorney-General's Department (**AGD**) is reviewing DVS access policies and is considering in particular potential privacy risks in expanding the range of businesses eligible for DVS access as may be permitted under the APPs.

We have provided a Privacy Impact Assessment report dated 15 May 2014 (**Attachment 4**) addressing the privacy benefits and risks associated with a greater number of private sector users having access to the DVS, in the context of the federal Privacy Act.

This Privacy Impact Assessment report addresses the privacy benefits and risks in the context of the privacy legislation and the evidence of identity documents legislation of each of the States and Territories.

For ease of reference, a glossary is provided in Schedule 1.

2. Executive summary

In short, we consider that expanded private sector access is legally permissible under the privacy legislation of each of the States and Territories and that privacy risks can be appropriately managed and mitigated in accordance with the recommendations in this report.

In our previous federal privacy impact assessment, we made the recommendations set out below.

2.1 Recommendations to mitigate the risk of unauthorised access or disclosure

In our previous federal privacy impact assessment, we made the following recommendations to mitigate the risk of unauthorised access or disclosure:

Recommendation 1

All prospective users must "opt in" to the Privacy Act to ensure that all users are required to comply with the Privacy Act.

Clause 11 of the DVS Business User Terms and Conditions of Use provides that "*You must ensure that your use of the DVS and Information Match Data complies with the Privacy Act 1988*". AGD has had a practice of ensuring that prospective DVS users have a privacy policy in place. However, with the expected increase in the number of private sector DVS users, AGD may not have capacity to continue this practice for all future applications. If Recommendation 1 is not adopted, there is a risk that a user who is not covered by the Privacy Act may argue that their use complies with the Privacy Act (not being required to meet certain conditions). The Gateway Service Provider Terms and Conditions of Use do not contain this provision. We recommend that the DVS Business User Terms and Conditions of Use and Gateway Service Provider Terms and Conditions of Use both be amended to include a condition to the effect that:

> ***"You agree to be bound by and comply with the Privacy Act 1988 (Cth) including the Australian Privacy Principles, in respect of your access to and use of the DVS and Information Match Data, whether or not the Privacy Act 1988 (Cth) would otherwise apply to you".***

We also recommend that users and GSPs be required to register their choice to be treated as organisations with the OAIC in accordance with s 6EA of the Privacy Act.

Recommendation 2

Each of the document issuing agencies, including the State and Territory agencies, should consider the privacy implications with respect to their participation in the DVS.

This recommendation has already been implemented by commissioning this report.

Recommendation 3

A review of the DVS be conducted 2 years after any expansion of access to the private sector that has regard to any complaints received, any security breaches identified or reported, and any known breaches of the Privacy Act.

This recommendation will allow participating agencies to ascertain whether there has been any unauthorised access or disclosure or misuse, interference and loss arising from the expansion of private sector access in practice and to identify any further reasonable measures that should be put in place to protect the information they hold.

Recommendation 4

No private sector organisation should be given access to the DVS unless its use of the DVS would comply with APP 9. In relation to APP 9.2(a), a private sector organisation will have a reasonable need to use the DVS in order to verify the identity of individuals for the purposes of its activities or functions if:

- **the prospective user's activities or functions in question are legitimate for that type of entity (assessed from the perspective of a reasonable person); and**
- **identification of an individual or being presented with the details of an evidence of identity document is reasonably necessary for the prospective user's activities or functions (assessed from the perspective of a reasonable person); and**
- **verification of the evidence of identity document - that is, use of the DVS - is reasonably necessary (assessed from the perspective of a reasonable person).**

Recommendation 5

Any revised access policy should contain clear, defensible criteria for giving a prospective user access to the DVS which should accord with the language of the statute. This would include:

- **the organisation cannot lawfully perform its legitimate functions or activities without verifying individuals' identity.**
- **the organisation has specific obligations to an agency or a State or Territory authority to verify identity.**
- **the prospective user has a responsibility to protect the public or some section of the public, and identification is reasonably necessary for that activity or function.**
- **it would not be reasonable to expect an organisation to perform its legitimate functions or activities without verifying individuals' identity.**

We note that the policy could specify classes of organisations that would meet the policy requirements, or provide that organisations with particular characteristics or functions would ordinarily meet the policy.

2.2 Recommendations to mitigate the risk of risk of misuse, interference and loss of personal information

In our previous federal privacy impact assessment, we made the following recommendations to mitigate the risk of misuse, interference or loss of personal information:

Recommendations 1 and 3 above mitigate against this risk.

Recommendation 6

There should be auditing of users' data security and privacy compliance in relation to their use of the DVS on at least a spot-check basis. Suspension or termination should be considered if a user has failed to report a data security or privacy breach to the DVS Hub Security Incident Investigator or the DVS Manager of which the organisation should reasonably have been aware, or if a user has reported a data security or privacy breach but has not put in place reasonable measures to ensure it is not repeated.

Recommendation 7

There should be a formal complaints process managed by AGD whereby individuals can complain to AGD about the actions of user organisations or GSPs in relation to their use of the DVS or use of information obtained though their use of the DVS. Users should be required to tell individuals where to find details of the complaints process. We recommend that the complaints process be detailed on the DVS website and also provide information as to other complaints mechanisms, such as the OAIC and State and Territory privacy regulators.

Recommendation 8

The operations of the DVS should be regularly reviewed and include consideration of any complaints received and reviews undertaken.

2.3 Recommendations to mitigate the risk that the individual has not provided free and informed consent to the DVS check

In our previous federal privacy impact assessment, we made the following recommendations to mitigate the risk that an individual has not consented to the DVS check:

Recommendation 7 above mitigates against this risk.

Recommendation 9

In order to ensure informed consent, users should be contractually required to provide individuals who present their document details for verification with an approved, concise plain English explanation of what the DVS does, how their details will be used, and what information will be contained in the DVS request by the user and response by the agency. Users should be required to tell individuals where they can find further information about the DVS, such as a page on the DVS website, so that consumers understand the nature of the DVS as well the benefits it provides.

At a minimum, we consider that users should be contractually required to tell individuals words to the effect of:

"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 webpage such as www.dvs.gov.au] or by

telephoning/writing to [insert telephone number, fax number or post office box number]".

Recommendation 10

Each user should be contractually required to provide the individual with a short, plain English explanation in the specific context of the prospective user organisation's activities or functions that addresses any alternatives to having their document details verified, the consequences if the individual does not consent to the DVS check (such as being unable to access the particular goods or services sought), and the consequences if the DVS returns a non-match response.

An example of this would be "*If you do not provide your driver's licence or passport number or your document is not verified by the Document Verification System, we may not be satisfied as to your identity and you may not be able to open an account with us online*".

The current Document Verification Service Business User Terms and Conditions of Use (**Attachment 2**) require that users obtain express and informed consent (clause 12). This recommendation could be implemented by amending clause 12.2 as follows:

"1.2 is informed of:

(a) the purpose for which that information is sought and will be used by you (including that the information will be subject to an Information Match Request in relation to relevant Official Record Holder information, and that a corresponding Information Match Result will be provided via the use of third party systems);

(b) any alternatives to the Information Match Request;

(c) any consequences if the individual does not consent to the Information Match Request; and,

(d) any consequences if the details in a Supported Document cannot be matched with the relevant Official Record Holder information."

Recommendation 11

There should be publicly available information on what individuals can do to access, and correct, information about them, including the contact details of the issuing agencies.

This recommendation could be implemented by ensuring that the DVS website contains the contact details of the issuing agencies.

2.4 Privacy risks specific to the individual States and Territories

Having now considered the applicable State and Territory privacy legislation, we consider that our existing recommendations are sufficient to mitigate the privacy risks of expanded private sector access. Accordingly, we have not made any additional recommendations.

We do note that each State and Territory will need to be satisfied as to legislative compliance. In particular, we note that a question arises as to whether a DVS request is to be regarded as a request for access to information extracted from the Register under applicable Births, Deaths and Marriages legislation. This is outside the scope of our privacy impact assessment but we would recommend that each State and Territory give consideration to whether a DVS request may fall within Part 7, Division 7.3 of the *Births, Deaths and Marriages Registration Act 1997* (ACT); Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1995* (NSW); Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act* (NT); Part 7 of the *Births, Deaths and Marriages Registration Act 2003* (QLD); Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (SA); Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1999* (TAS); Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (VIC); or Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1998* (WA) respectively and, if so, whether document verification through the

DVS complies with the applicable provisions. We would also recommend that each State and Territory (other than New South Wales, Queensland and Victoria) give consideration to whether driver licensing legislation should make specific provision for participation in the DVS.

3. About this PIA

3.1 What is a privacy impact assessment?

A Privacy Impact Assessment, or **PIA**, is an examination of a project from a privacy perspective. The primary purposes of a PIA are to:

a) examine how personal information is collected, used and disclosed as part of a project;

b) analyse the impacts of the project on personal privacy; and

c) identify and recommend options for managing, reducing or removing those impacts.

PIAs are conducted to ensure that privacy issues are fully considered in the design and implementation phase of a project. PIAs help ensure that projects meet privacy requirements in legislation and are also consistent with broader community privacy expectations.

3.2 The approach of this PIA

Our previous PIA (**Attachment 4**) was prepared broadly in accordance with the *Privacy Impact Assessment Guide* (Office of the Australian Information Commissioner, May 2010) (the **PIA Guide**). That guide recommends that PIAs be conducted in five key stages, as shown diagrammatically below.

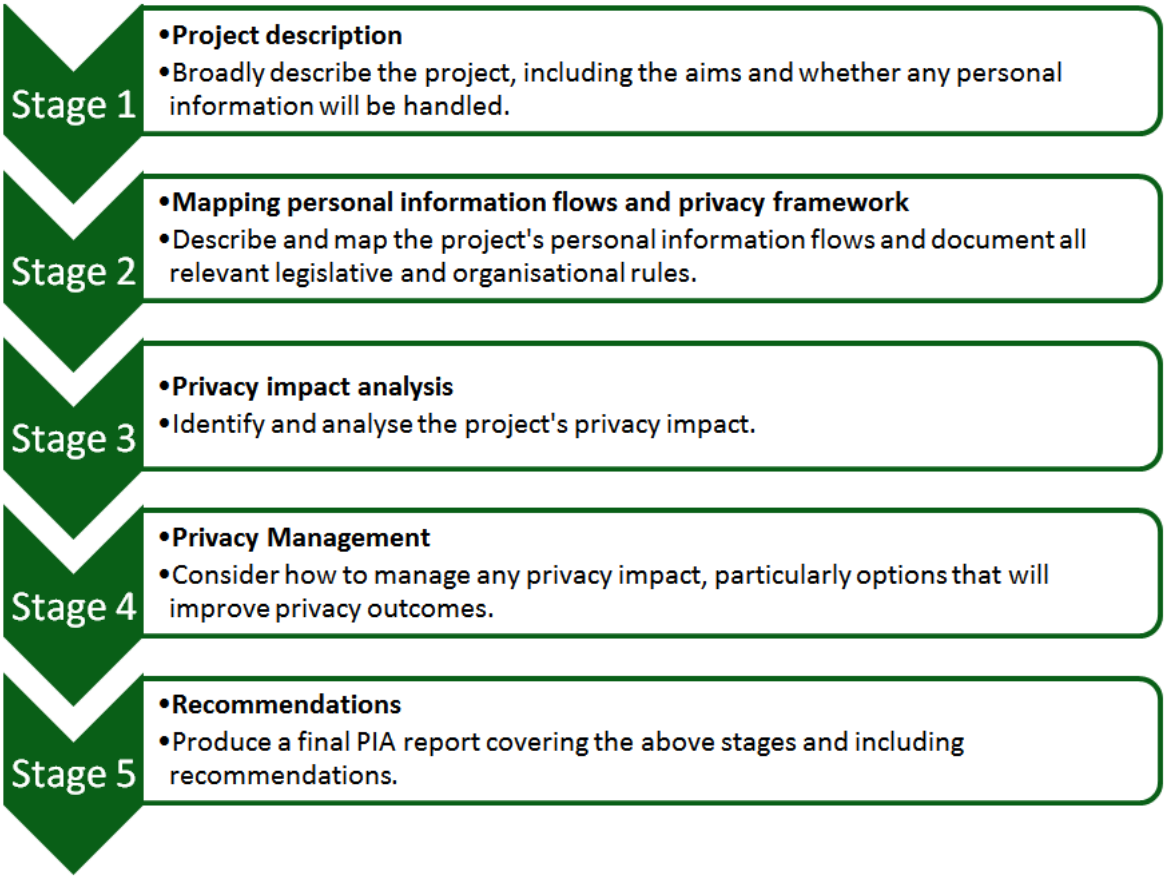


Figure 1—PIA stages (Source: PIA Guide, p xii)

This PIA expanded the scope of the original PIA to consider the legislation relevant to privacy and evidence of identity documents of each of the States and Territories. This PIA then considered whether the original recommendations made with regard to the federal Privacy Act would be adequate to meet the obligations imposed in the context of each State and Territory.

3.3 Relevant Documents

We had the benefit of reading the documents set out in Schedule 2.

We also had the benefit of reading written submissions prepared following the consultation process described at 3.4 below.

3.4 Consultation

In the course of our previous PIA at **Attachment 4**, we consulted with the AGD, the OAIC, government document issuing agencies, users of the DVS (including government agencies and prospective private sector organisation users), and privacy experts and advocacy groups.

For the purposes of this national PIA, we extended this consultation process to relevant State and Territory government agencies and privacy commissioners, being:

a) the Australian Capital Territory Directorate of Justice and Community Safety and (in respect of the Territory's privacy laws) the Office of the Australian Information Commissioner;

b) the New South Wales Department of Police and Justice, Information and Privacy Commission, Attorney-General's Department and Transport for NSW;

c) the Northern Territory Department of the Attorney-General and Justice and the Office of the Information Commissioner;

d) the Queensland Department of the Premier and Cabinet and the Office of the Information Commissioner;

e) the South Australian Attorney-General's Department, Department of Planning, Transport and Infrastructure and Birth Deaths and Marriages and Privacy Committee of South Australia;

f) the Tasmanian Department of Premier and Cabinet and the Ombudsman;

g) the Victorian Registry of Births, Deaths and Marriages, Department of Justice, VicRoads and Privacy Victoria; and

h) the Western Australian Registry of Births, Deaths and Marriages and Department of Finance.

We did this by emailing the written invitation to comment at **Attachment 1** to relevant State and Territory government agencies and privacy commissioners on 4 June 2014. We then met with relevant State and Territory government agencies on 10 June 2014 (by video conference). We invited those consulted to provide comments or submissions by 18 June 2014 if possible.

We also emailed the written invitation to comment at **Attachment 1** to private sector organisations, Gateway Service Providers, independent advocacy groups and privacy experts who were consulted in the course of the previous PIA, including Veda, Edentiti, the Commonwealth Bank, Telstra, the Australian Privacy Foundation, Electronic Frontiers Australia and Liberty Victoria. We invited them to provide any further comments or submissions in the context of any particular States or Territories, or generally.

We asked the following questions:

- In addition to the DVS, what other methods (paper-based, electronic, etc) can organisations use to verify the identity of individuals?
- What might be the privacy impacts of those other identity verification processes (document copying, record keeping, etc)?
- Taking into account the existing controls on DVS access, what do you consider to be the current level of privacy risk associated with DVS use by government agencies and other eligible organisations?
- Can you identify any potential scenarios in which these risks might materialise?
- What impact does your State or Territory's privacy regime have on the lawfulness of the proposal?
- What impact does your State or Territory's laws relating to the handling of information on evidence of identity documents (such as driver licences, birth certificates and marriage certificates) have on the lawfulness of the proposal?
- In what circumstances could the proposal have a positive privacy impact for individuals whose identities are being verified by an organisation?
- In what circumstances could the proposal have a negative privacy impact for individuals whose identities are being verified by an organisation?
- In what ways could any negative privacy impacts be managed?
- What additional security or access controls should be adopted if the proposal is adopted?
- What information should individuals be given about DVS transactions if the proposal is adopted?
- What identity verification obligations or authorities currently apply to private sector organisations in your State or Territory under either:
- State and Territory legislation; or
- other non-legislative arrangements managed by State or Territory government agencies?
- Please also address any other issues you see with the proposals

We acknowledge with gratitude the written submissions we received from agencies, users and privacy experts in the course of this PIA and our previous PIA.

4. Description of the DVS

4.1 Evidence of Identity Documents

There are a range of documents verified by the DVS which commonly serve as "identity documents" in the community. We note that it was submitted to us by a number of individuals or organisations consulted that it is convenient but incorrect to describe these documents as identity documents. As the documents verified contain information that commonly functions for identifying purposes, such as driver's licences, and passports, in this document we will refer to **evidence of identity documents**.

The DVS does not verify that a document presented is authentic. Rather, it confirms that the details contained (or said to be contained) in the document match (or do not match) the details held by the agency that issued the document.

4.2 Background

In 2005, the Council of Australian Governments (**COAG**) endorsed the development of a National Identity Security Strategy (**NISS**) to protect the Australian community from identity theft. In doing so COAG also agreed to establish a Document Verification Service (DVS) to combat the misuse of false and stolen identities.

One of the primary aims of the NISS in establishing the DVS was to ensure that government agencies could confirm that the details of an evidence of identity document issued by another agency were correct. The DVS does not confirm whether a document is genuine or not but it does confirm that the information contained in the document matches the information held by the document issuing agency.

The DVS has been available to some government agencies (principally Commonwealth agencies) since 2008.

Since December 2013, the DVS has been available to those private sector organisations that are required under Commonwealth law to know the identity of their customers, primarily organisations involved in banking, credit reference, finance, superannuation, telecommunications, and gambling. Legislation that requires organisations to identify their customers includes:

a) Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth);

b) Financial Transactions Reports Act 1988 (Cth) and Financial Transactions Reports Regulations 1990 (Cth);

c) Superannuation Industry (Supervision) Act 1993 (Cth) and Superannuation Industry (Supervision) Regulations 1994 (Cth);

d) Retirement Savings Account Act 1997 (Cth) and Retirement Savings Account Regulations 1997 (Cth);

e) The former Credit Reporting Code of Conduct under the Privacy Act and now the Privacy (Credit Reporting) Code 2014 (Version 1.2) (**CR Code**);

f) Aviation Transport Security Act 2004 (Cth) and Aviation Transport Security Regulations 2005 (Cth);

g) Maritime Transport and Offshore Facilities Security Act 2003 (Cth) and Maritime Transport and Offshore Facilities Security Regulations 2003 (Cth); and

h) Telecommunications Act 1997 (Cth) and Telecommunications (Service Provider - Identity Checks for Prepaid Mobile Carriage Services) Determination 2013 (Cth).

Since December 2013, the DVS has also been available to approved GSPs. GSPs act as agents for users, either allowing approved users to search the DVS through the GSP's interface (DVS application) or conducting both the customer identification and the technical transactions on behalf of users. GSPs allow users to avoid the expense of developing their own DVS interface and complying with security protocols. GSPs also facilitate cheaper search fees under a volume discount - the general access rate being $1.40 per search with volume-based discounting reducing that cost to between $0.65 - $1.20.

Government agencies and GSPs have their own interfaces with the DVS. Private sector organisations may have direct access to the DVS through their own interface or may use the services of a GSP.

The governance arrangements are summarised in the *Document Verification Service: An Overview* (V4 December 2013). The contractual terms of access are contained in the Document Verification Service Business User Terms and Conditions of Use (**Attachment 2**) and Document Verification Service Gateway Service Provider Terms and Conditions of Use (**Attachment 3**) and are summarised in Schedule 4. We understand that the instructions and guidance provided by the AGD (that GSPs must comply with pursuant to clause 10 of the Gateway Service Provider Terms and Conditions of Use, and users must comply with pursuant

to clause 7 of the Business User Terms and Conditions of Use) currently include the DVS Supporting Materials.

All DVS users including private sector organisations must be approved by the DVS Advisory Board. The DVS Advisory Board currently undertakes a due diligence process before approving private sector users, to confirm that the prospective user is covered by the Privacy Act, has customer identification obligations under law, and has its registration or licensing overseen by local regulatory authorities such as the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Prudential Regulation Authority (APRA), Australian Securities and Investments Commission (ASIC) or the Australian Communications and Media Authority (ACMA).

On 5 May 2014, the Attorney-General, Senator the Hon George Brandis QC, launched the DVS commercial service at the CeBIT Australia Conference. AGD is currently considering the privacy implications of a greater number of private sector organisations requesting access to the DVS following the introduction of the new APPs which took effect 12 March 2014 pursuant to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

4.3 What is the DVS?

The DVS is a secure online system that enables organisations to verify the information contained in evidence of identity documents with the records of the document issuing agencies (such as Commonwealth agencies and State and Territory Registries). The evidence of identity documents that can be verified against the records of the issuing agencies include:

a) birth certificates;

b) certificates of registration by descent;

c) change of name certificates;

d) citizenship certificates;

e) driver licenses;

f) marriage certificates;

g) Medicare cards;

h) passports;

i) Immi Cards; and

j) visas.

The DVS is not a database and does not itself store any personal information for any longer than is required to complete the search.

The DVS is available 24 hours per day, 7 days per week and generally provides a response within a few seconds.

4.4 What is the information flow?

There are five participants in a DVS transaction:

a) **The individual—**The individual wishes to access or obtain a benefit, product or service from a user organisation. To do so, he or she must provide evidence of their identity in the form of the physical document, a copy of the document or the details of an evidence of identity document. This is done online, by telephone, in writing or in person.

b) **The user—**The user enters the details of the evidence of identity document (either directly or through a GSP - see below) into a DVS system or interface. The details are entered manually and then the request is sent securely by the user's interface to the DVS Hub.

c) **The gateway service provider (optional)—**The GSP allows users to interrogate the DVS through the GSP's interface (or DVS system). The GSP acts as the agent of the user.

d) **The DVS Hub**—The DVS Hub accepts the request from the user (or their GSP) using the Verification/Match Request Number (**VRN**) assigned by the user (or their GSP). The DVS Hub reformats and reroutes the request to the appropriate issuing agency with a new VRN. The DVS Hub receives a Y, N, S or D response back from the issuing agency with the second VRN. The DVS Hub then reformats and reroutes the response back to the user with the original VRN.

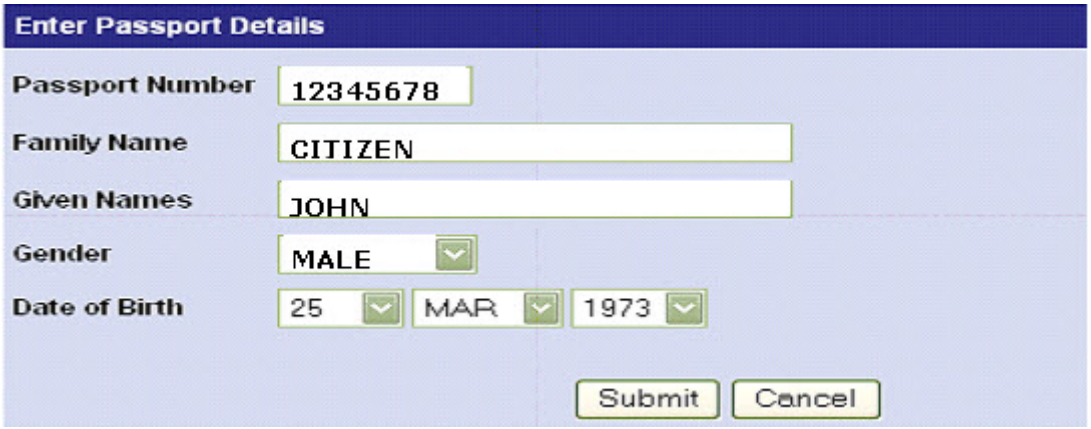
e) **The government document issuing agency**—The issuing agency receives the request from the DVS Hub, conducts an automated check of the details in the request against its own records, and sends a response to the DVS Hub being Y, N, S or D.

A search of the DVS involves the following steps:

- An individual provides the details of an identity document to establish his or her identity, either by presenting the physical document or a copy of the document, by providing the details by telephone or online, or by setting out the details in a written application. The individual consents to a DVS user checking the details of the identity document.

- The DVS user then enters the details of the identity document (for example, the passport number, family name, first name, gender and date of birth) into the DVS/The DVS user provides the details to the DVS via a GSP.

The following example is provided on the DVS website:



- The request is then sent to the DVS Hub, which is a technical router that allows DVS requests to be securely sent between users and issuing agencies, through a secure communications route.

- The DVS Hub encrypts the request and forwards it via a different secure communications route to the document issuing agency. A transaction number is assigned to it.

- The document issuing agency undertakes an automated check of the agency's data to ascertain whether the information provided matches the information held by the agency.

- The document issuing agency sends a response back to the DVS Hub via the same secure communications route as the request from the DVS.
- The DVS Hub re-encrypts the response and sends back to the user (or GSP) via the original secure communications route.
- The user will receive one of the following responses in respect of the entire request:
    - [**Y**] – all of the details entered match the details of the issuing agency's records and the document is still valid (that is, not expired or cancelled).
    - [**N**] – one or more of the details do not match the details of the issuing agency's records or the details match but the document is no longer valid (that is, it has expired or it has been cancelled).
    - [**S**] - system availability error. The DVS request cannot be sent to the issuing agency within 60 seconds or a system availability problem prevents the response being returned. A user should resubmit the request at a later time.
    - [**D**] - data range error. This indicates that the request includes data that has not been electronically captured by the issuing agency. For example, older documents may not have been electronically captured in particular jurisdictions.

5. What is proposed in terms of expanded private sector access?

The DVS is already available to private sector organisations with a legislated requirement under Commonwealth legislation to identify their customers. The AGD anticipates that the reforms to the Privacy Act will lead to a greater number of private sector organisations requesting access.

Expanded use of the DVS offers significant privacy benefits over more intrusive identity verification methods, avoiding the need for organisations to keep copies of evidence of identity documents. Expanded DVS use is also likely to facilitate online transactions without the need for hardcopy evidence of identity documents to be provided.

However, the AGD and the issuing agencies must comply with federal, State and Territory legislation.

In our previous PIA, we consider compliance with the APPs in the federal Privacy Act. This PIA considers applicable State and Territory legislation.

5.1 What types of organisations may request access to the DVS?

Potentially, any private sector organisation might see a benefit in verifying evidence of identity documents through the DVS.

In the course of previous consultation, a number of examples were suggested to us which include:

- utilities providers, to whom customers must provide "acceptable identification" under National Energy Retail Rules;
- the real estate sector, in the context of assessing the suitability of tenants, and especially in the context of the Australian Registrars' National E-Conveyancing Council (**ARNECC**) and the implementation of the regulatory framework for National E-Conveyancing (the Electronic Conveyancing National Law);

- sensitive employment environments;
- universities and other education providers (in the context of avoiding plagiarism and cheating);
- registration of health professionals;
- second hand goods dealers;
- car rentals and car share arrangements;
- hotels with safety deposit boxes and gaming machines;
- child protection;
- personnel screening agencies;
- online dating; and
- online gambling.

6. National Privacy Impacts

In our previous PIA, we concluded that expanded private sector access was legally permissible. We identified that the major privacy risks were:

- The risk of unauthorised access or disclosure;
- The risk of misuse, interference or loss of personal information; and
- The risk that an individual has not provided free and informed consent to a DVS check and the disclosure of their personal information in the course of the DVS check.

We concluded that each of these risks could be appropriately managed and mitigated in accordance with the recommendations in our PIA.

We have now considered the privacy and evidence of identity document legislation in each of the eight States and Territories. We consider that expanded private sector access is legally permissible in each of the States and Territories. In our view, the same key privacy risks arise in each State and Territory. In our view, there are no additional privacy risks that arise in the States and Territories and our existing recommendations are sufficient to mitigate against the privacy risks in each jurisdiction.

7. The Australian Capital Territory

7.1 Privacy

Privacy in the Australian Capital Territory is currently governed by the *Information Privacy Act 2014* (ACT) which commenced on 11 September 2014, replacing the *Privacy Act 1998* (Cth) as at 1 July 1994 and as modified by the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth) which previously applied to ACT public sector agencies.

Under the *Information Privacy Act 2014* (ACT) a public sector agency (which includes the Office of Regulatory Services and Territory and Municipal Services: s 9) must not do an act or engage in a practice that breaches a Territory Privacy Principle (**TPP**): s 20. The TPPs largely

replicate the APPs, save that they do not include provisions relating to private sector and other entities: see note 3 to Schedule 1.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in the Australian Capital Territory.

7.2 Evidence of identity documents

The Office of Regulatory Services - Births, Deaths and Marriages is responsible for birth certificates, change of name certificates and marriage certificates in accordance with the *Births, Deaths and Marriages Registration Act 1997* (ACT). In "*providing information extracted from the register, the registrar-general must, as far as practicable, protect a person to whom the entry in the register relates from unreasonable intrusion into his or her privacy*": section 44. In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 7, Division 7.3 of the *Births, Deaths and Marriages Registration Act 1997* (ACT). Section 42(1)(b) provides that a person may apply to the registrar-general for the provision from the register of the information stated in the application. Section 42(2) provides that the registrar-general may give the applicant any of the stated information that is available if satisfied that the applicant has an adequate reason for wanting the information (and must, in that context, have regard to the nature of the applicant's interest, the sensitivity of the information to be provided and the use to be made of the information) and the giving of the information is in accordance with the statement of policies under s 46. We note that the existing Certificate Access Policy under s 46 does not provide for verification of the details of identity documents.

We note that documents issued by the Office of Regulatory Services can already be verified through the Certificate Validation Service so, in our view, the expansion of private sector access does not increase the risk of possible non-compliance with s 42. However, in our view the Territory should consider whether a DVS request would fall within s 42 and, if so, whether the Certificate Access Policy ought to be amended to specifically provide for document verification through the DVS.

Territory and Municipal Services is responsible for the driver licence register in accordance with the *Road Transport (Driver Licensing) Act 1999* (ACT). Section 9 of that Act provides that the "road transport authority must ensure that information in the driver licence register or demerit points register is kept securely and disclosed only in accordance with this Act or another law in force in the ACT". In our view, DVS checks carried out in compliance with the *Information Privacy Act 2014* (ACT) will satisfy this obligation. The Territory may wish to give consideration to whether specific provision should be made for participation in the DVS.

7.3 Conclusion in respect of the Australian Capital Territory

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in the Australian Capital Territory.

In our view, the Office of Regulatory Services should give further consideration to whether a DVS request may fall within Part 7, Division 7.3 of the Births, Deaths and Marriages Registration Act 1997 (ACT) and, if so, whether the Certificate Access Policy ought to be amended to specifically provide for document verification through the DVS.

8. New South Wales

8.1 Privacy

We note the Information and Privacy Commission's view that, assuming that the DVS continues to operate on a consent basis the *Privacy and Personal Information Protection Act 1998* (NSW) is not a barrier to expanded private sector access. We agree with this view.

New South Wales public sector agencies must not do any thing, or engage in any practice, that contravenes an information protection principle: s 21. Like APP 11, the information protection principles in New South Wales require that information held by New South Wales public sector agencies is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse: s 12(c). A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless (inter alia) the individual to whom the information relates has consented to the use of the information for that other purpose, or the other purpose for which the information is used is directly related to the purpose for which the information was collected: s 17.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in New South Wales.

8.2 Evidence of identity documents

The Registry of Births, Deaths & Marriages within the Department of Justice is responsible for birth certificates, change of name certificates and marriage certificates in accordance with the *Births, Deaths and Marriages Registration Act 1995* (NSW).

Section 48 of the Act provides that in "*providing information extracted from the Register, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy*". In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1995* (NSW). Section 46(1)(b) provides that the Registrar may provide a person or organisation that has an adequate reason for wanting information from the Register with information extracted from the Register. Section 46(2) provides that in deciding whether an applicant has an adequate reason for wanting information extracted from the Register the Registrar must have regard to the nature of the applicant's interest, the sensitivity of the information, the use to be made of the information and other relevant factors. Section 46(3) provides that in deciding the conditions on which information extracted from the Register, is to be given under the section, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy. We have no knowledge as to whether the Registrar has decided that verifying documents via a DVS check represents an adequate reason for wanting the information extracted from the Register.

We note that documents issued by Registry of Births, Deaths & Marriages can already be verified through the Certificate Validation Service so, in our view, the expansion of private sector access does not increase the risk of possible non-compliance with s 46. However, we consider that New South Wales should consider whether a DVS request would fall within Part 8, Division 4 and, if so, whether document verification through the DVS complies with s 46.

Roads and Maritime Services is responsible for the driver licence register in accordance with the *Road Transport Act 2013* (NSW). Section 30 of that Act provides that Roads and Maritime Services must ensure that information contained in the driver licence register that is of a personal nature or that has commercial sensitivity for the person about whom it is kept is not

released except as provided by the statutory rules or under another law. The statutory rules specifically provide that Roads and Maritime Services may participate in the DVS: *Road Transport (Driver Licensing) Regulation 2008* (NSW) regulation 109A.

8.3 Conclusion in respect of New South Wales

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in New South Wales.

In our view, the Registry of Births, Deaths & Marriages should consider whether a DVS request would fall within Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1995* (NSW) and, if so, whether document verification through the DVS complies with s 46.

9. The Northern Territory

9.1 Privacy

Privacy in the Northern Territory is governed by the *Information Act* (NT). It is an interference with a person's privacy if a Northern Territory public sector organisation contravenes an information privacy principle set out in Schedule 2 (**IPP**): s 67. IPP 2.1 provides that a public sector organisation must not use or disclose personal information about an individual for a secondary purpose unless (inter alia) the secondary purpose is related to the primary purpose and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose, or the individual consents to the use or disclosure of the information, or the use or disclosure is required or authorised by law. IPP 4.1 provides that a public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

The Northern Territory Information Commissioner has raised concerns about the risk of misuse (such as high speed automated queries, and use of the DVS to *obtain* rather than *verify* information held about an individual) increasing commensurate with increased private sector access. We share this concern but consider that this risk is adequately mitigated by our existing recommendations 1, 3, 6, 7 and 8.

We note the Northern Territory Information Commissioner's view that reasonable steps are currently in place to minimise privacy risks but that, as the DVS is not regulated, there is a risk that those steps will not be maintained for the life of the DVS. If users and GSPs continue to gain access to the DVS according to the Terms and Conditions of Use, and if auditing measures are put in place, we are comfortable that the structures will be in place to protect privacy.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in the Northern Territory.

9.2 Evidence of identity documents

The Department of the Attorney-General and Justice - Births, Deaths and Marriages is responsible for birth certificates, change of name certificates, marriage certificates in accordance with the *Births, Deaths and Marriages Registration Act* (NT).

Section 43 of the Act provides that in "*providing information extracted from the Register, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy* ". In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act* (NT). Section 41(1)(b) provides that the Registrar may provide a person or organisation that has an adequate reason for wanting information from the Register with information extracted from the Register. Section 41(2) provides that in deciding whether an applicant has an adequate reason for wanting information extracted from the Register the Registrar must have regard to the nature of the applicant's interest, the sensitivity of the information, the use to be made of the information and other relevant factors. Section 41(3) provides that in deciding the conditions on which information extracted from the Register is to be given under the section, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy. We have no knowledge as to whether the Registrar has decided that verifying documents via a DVS check represents an adequate reason for wanting the information extracted from the Register.

We consider that the Northern Territory should consider whether a DVS request would fall within Part 7, Division 4 and, if so, whether document verification through the DVS complies with s 41.

The Department of Transport - Motor Vehicle Registry is responsible for the driver licence register in accordance with -*Motor Vehicles Act 1949* (NT). We do not consider that anything in this Act is an impediment to the expansion of private sector access to the DVS. However, the Territory may wish to give consideration to whether specific provision should be made for participation in the DVS.

9.3 Conclusion in respect of the Northern Territory

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in the Northern Territory.

In our view, the Department of the Attorney-General and Justice - Births, Deaths and Marriages should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act* (NT) and, if so, whether document verification through the DVS complies with s 41.

10. Queensland

10.1 Privacy

Privacy in Queensland is governed by the *Information Privacy Act 2009* (QLD). We note the Office of the Information Commissioner's view that the privacy risks arising out of expanded public sector access are the same as the current privacy risks.

Queensland agencies must comply with the Information Privacy Principles (**IPPs**) at Schedule 3 to the *Information Privacy Act 2009* (QLD): s 27. IPP 4(1) provides that an agency having control of a document containing personal information must ensure that the document is protected against loss, unauthorised access, use, modification or disclosure and any other misuse. IPP 11(1) provides that an agency having control of a document containing an individual's personal information must not disclose the personal information to an entity, other than the individual the subject of the personal information, unless (inter alia) the individual is reasonably likely to have been aware, or to have been made aware (see IPP 2), that it is the agency's usual practice to disclose that type of personal information to the relevant entity or the individual has expressly or impliedly agreed to the disclosure or the disclosure is authorised or required under a law.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in Queensland.

10.2 Evidence of identity documents

The Department of Justice and Attorney-General - Births, Deaths and Marriages is responsible for birth certificates and change of name certificates pursuant to the *Births, Deaths and Marriages Registration Act 2003* (QLD).

Section 46 of the Act provides that, in giving or allowing an entity to obtain information contained in the register, the "*registrar must, as far as practicable, protect the persons to whom the information relates from unjustified intrusion on their privacy*". In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 7 of the *Births, Deaths and Marriages Registration Act 2003* (QLD). Section 44 deals with requests for information on the register and provides that unless the request relates to historical information, the Registrar may refuse the application if the applicant does not have an adequate reason for requesting the information, having regard to the relationship (if any) between the applicant and the person to whom the information relates, the reason that the applicant wants the information, the use to be made of the information, the age of the entry, the contents of the entry, the sensitivity of the information and other relevant factors. Section 45 provides that the Registrar may allow an entity to obtain information contained in a register other than under s 44 and that the Registrar must maintain written information policies relating to who may obtain information under this section. The current Certificate Access Policy does not provide for electronic verification of records.

We note that documents issued by the Department of Justice and Attorney-General - Births, Deaths and Marriages can already be verified through the Certificate Validation Service (other than Queensland marriage certificates) so, in our view, the expansion of private sector access does not increase the risk of possible non-compliance with ss 44 and 45. However, we consider that should Queensland consider whether a DVS request would fall within Part 7 and, if so, whether document verification through the DVS complies with ss 44 and 45.

The Department of Transport and Main Roads is responsible for the driver licence register pursuant to the *Transport Operations (Road Use Management) Act 1995* (QLD). We note the Department's view that there is no legislative impediment under that Act to the expansion of private sector access to the DVS. We agree with that view. Section 77(1) of the *Transport Operations (Road Use Management) Act 1995* (QLD) provides that:

> *The chief executive may release, in writing or electronically, information kept under this Act about a person's prescribed authority [defined to mean a Queensland driver's licence: Schedule 4] or traffic history to—*
>
> *…*
>
> *(d) an entity that, under an agreement between the State and other governments, maintains a database containing information about driver licences and traffic histories.*

We agree with the Department's view that this authorises participation in the DVS.

10.3 Conclusion in respect of Queensland

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in Queensland.

In our view, the Department of Justice and Attorney-General - Births, Deaths and Marriages should consider whether a DVS request would fall within Part 7 of the *Births, Deaths and*

Marriages Registration Act 2003 (QLD) and, if so, whether document verification through the DVS complies with ss 44 and 45.

11. South Australia

11.1 Privacy

Privacy in South Australia is governed by the *Information Privacy Principles Instruction* (SA).

South Australian government agencies must comply with the Information Privacy Principles (**IPPs**) at Part II to the *Information Privacy Principles Instruction* (SA). IPP 4 provides that an agency should take reasonable steps to ensure that personal information is not misused. IPP 10 provides that an agency should not disclose personal information for a secondary purpose unless (inter alia) the record-subject would reasonably expect the agency to disclose the information for the secondary purpose that is related to the primary purpose, the record-subject has expressly or impliedly consented, or the disclosure is authorised or required under a law.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in South Australia.

11.2 Evidence of identity documents

The Attorney-General's Department - Births, Deaths and Marriages Registration Office is responsible for birth certificates, change of name certificates and marriage certificates pursuant to the *Births, Deaths and Marriages Registration Act 1996* (SA).

Section 45 of the Act provides that in "*providing information extracted from the Register, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy*". In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (SA). Section 43(1)(b) provides that the Registrar may provide a person or organisation that has an adequate reason for wanting information from the Register with information extracted from the Register. Section 43(2) provides that in deciding whether an applicant has an adequate reason for wanting information extracted from the Register the Registrar must have regard to the nature of the applicant's interest, the sensitivity of the information, the use to be made of the information and other relevant factors. Section 43(3) provides that in deciding the conditions on which information extracted from the Register, is to be given under the section, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy. We have no knowledge as to whether the Registrar has decided that verifying documents via a DVS check represents an adequate reason for wanting the information extracted from the Register.

We consider that South Australia should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (SA) and, if so, whether document verification through the DVS complies with s 43.

The Department of Planning, Transport and Infrastructure - Motoring is responsible for the driver licence register pursuant to the *Motor Vehicles Act 1959* (SA). We do not consider that anything in this Act is an impediment to the expansion of private sector access to the DVS. However, South Australia may wish to give consideration to whether specific provision should be made for participation in the DVS.

11.3 Conclusion in respect of South Australia

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in South Australia.

In our view, the Attorney-General's Department - Births, Deaths and Marriages Registration Office should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (SA) and, if so, whether document verification through the DVS complies with s 43.

12. Tasmania

12.1 Privacy

Privacy in Tasmania is governed by the *Personal Information Protection Act 2004* (TAS).

Personal information custodians (defined to include public authorities: s 3) must comply with the personal information protection principles specified in Schedule 1: s 17. The personal information protection principles include principle 2, that the personal information custodian must not disclose personal information for a secondary purpose unless (inter alia) the secondary purpose is related to the primary purpose and the individual would reasonably expect the information to be disclosed for the secondary purpose, or the individual has consented, or the disclosure is authorised or required by or under law. Principle 4 provides that a personal information custodian must take reasonable steps to protect the personal information from misuse, loss, unauthorised access, modification or disclosure. Principle 9 provides that personal information may only be disclosed outside Tasmania if the personal information custodian reasonably believes that the recipient is subject to a law, biding scheme or contract that has principles for the fair handling of the information that are substantially similar to the personal information protection principles.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in Tasmania.

12.2 Evidence of identity documents

The Department of Justice - Births, Deaths and Marriages is responsible for birth certificates, change of name certificates, marriage certificates pursuant to the *Births, Deaths and Marriages Registration Act 1999* (TAS);

Section 45 of the Act provides that in "*providing information extracted from the Register, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy*". In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1999* (TAS). Section 43(1)(b) provides that the Registrar may provide a person or organisation that has an adequate reason for wanting information from the Register with information extracted from the Register. Section 43(2) provides that in deciding whether an applicant has an adequate reason for wanting information extracted from the Register the Registrar must have regard to the nature of the applicant's interest, the sensitivity of the information, the use to be made of the information and other relevant factors. Section 43(3) provides that in deciding the conditions on which information extracted from the Register, is to be given under the section, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy. We have no knowledge as to whether the Registrar has decided that verifying documents via a DVS check represents an adequate reason for wanting the information extracted from the Register.

We consider that Tasmania should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1999* (TAS) and, if so, whether document verification through the DVS complies with s 43.

The Department of State Growth - Transportis responsible for the driver licences register pursuant to the *Vehicle and Traffic Act 1999* (Tas). Regulation 125 of the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (TAS) specifically provides for NEVDIS but not for the DVS. Regulation 125(2) provides:

> *(2) The Registrar may divulge protected information only in the following circumstances:*
>
> *(a) if and as the Registrar considers appropriate in the public interest for the purposes of the administration of an Act of this State, another State or a Territory, or the Commonwealth;*
>
> *(b) if and as authorised by the person to whom the information relates;*
>
> *(c) if and as required by a court or other body or person authorised to take evidence;*
>
> *(d) if and as required for the purposes of NEVDIS;*
>
> *(e) if and as authorised by administrative guidelines issued by the Minister;*
>
> *(f) if and as otherwise authorised by the Minister.*

In our view, the Department of Infrastructure, Energy and Resources - Transport should consider whether regulation 125 of the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (TAS) should specifically include the DVS.

12.3 Conclusion in respect of Tasmania

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in Tasmania.

In our view, the Department of Justice - Births, Deaths and Marriages should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1999* (TAS) and, if so, whether document verification through the DVS complies with s 43.

In our view, the Department of State Growth - Transport should consider whether regulation 125 of the *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (TAS) should specifically include the DVS.

13. Victoria

13.1 Privacy

Privacy in Victoria is governed by the *Privacy and Data Protection Act 2014* (VIC) . Organisations (defined to include public sector agencies: s3 and s13) must not do an act or engage in a practice that contravenes an Information Privacy Principle (**IPP**) in Schedule 1: s20(1). Specifically under the Victorian Act, public sector agencies must in administering a public register, so far as is reasonably practicable, not do an act or engage in a practice that contravenes an Information Privacy Principle (**IPP**): s20(2).

IPP 2.1 provides that an organisation must not use or disclose personal information about an individual for a secondary purpose unless (inter alia) the secondary purpose is related to the primary purpose and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose, or the individual consents to the use or

disclosure of the information, or the use or disclosure is required or authorised by law. IPP 4.1 provides that a public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

We acknowledge Privacy Victoria's concern about the potential for over-regulation in the community if private sector access is broadly extended. In our view, this concern can be dealt with in the development of a robust access policy in accordance with our Recommendations 4 and 5.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in Victoria.

13.2 Evidence of identity documents

The Department of Justice and Regulations - Births, Deaths & Marriages is responsible for birth certificates, change of name certificates and marriage certificates pursuant to the *Births, Deaths and Marriages Registration Act 1996* (VIC). In "*providing information extracted from the Register, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy*": section 44. In our view, existing measures, including the fact that the information is only verified with a "Y" or "N" response (rather than the correct answer being provided where the records do not match) together with the fact that, in most cases, the DVS request will have been carried out with the consent of the person to whom the entry in the register relates (it being otherwise a breach of the terms and conditions of use) will satisfy this provision.

In our view, a DVS request may fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (VIC). Section 48(1)(b) provides that the Registrar may provide a person or organisation that has an adequate reason for wanting information from the Register with information extracted from the Register. Section 48(2) provides that in deciding whether an applicant has an adequate reason for wanting information extracted from the Register the Registrar must have regard to the nature of the applicant's interest, the sensitivity of the information, the use to be made of the information and other relevant factors. Section 48(3) provides that in deciding the conditions on which information extracted from the Register, is to be given under the section, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy. We have no knowledge as to whether the Registrar has decided that verifying documents via a DVS check represents an adequate reason for wanting the information extracted from the Register.

We consider that Victoria should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (VIC) and, if so, whether document verification through the DVS complies with s 48.

The Department of Economic Development, Jobs, Transport and Resources - VicRoads is responsible for the driver licence register pursuant to the *Road Safety Act 1986* (VIC). We do not consider that anything in this Act is an impediment to the expansion of private sector access to the DVS. Section 90M(1) specifically provides that the Roads Corporation may verify information contained in a driver licence or learner permit if that information is provided to a public sector body or private sector body as evidence of an individual's identity.

13.3 Conclusion in respect of Victoria

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in Victoria.

In our view, the Department of Justice and Regulations - Births, Deaths & Marriages should consider whether a DVS request would fall within Part 7, Division 4 of the *Births, Deaths and Marriages Registration Act 1996* (VIC) and, if so, whether document verification through the DVS complies with s 48.

14. Western Australia

14.1 Privacy

There is no dedicated privacy legislation in Western Australia. Rather, some of the privacy principles are provided for in the *Freedom of Information Act 1992* (WA) and various agency-specific provisions.

In our view, existing measures together with the recommendations in our first PIA are adequate to mitigate the privacy risks in Western Australia.

14.2 Evidence of identity documents

The Department of the Attorney General - Registry of Births, Deaths & Marriages is responsible for birth certificates, change of name certificates, marriage certificates in accordance with the *Births, Deaths and Marriages Registration Act 1998* (WA). Section 56 provides that in "*providing information extracted from the Register, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy*".

In our view, a DVS request may fall within Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1998* (WA). Section 54(1)(b) provides that the Registrar may provide a person having an adequate reason for wanting information from the Register with information extracted from the Register. Section 54(2) provides that in deciding whether an applicant has an adequate reason for wanting information extracted from the Register the Registrar must have regard to the nature of the applicant's interest, the sensitivity of the information, the use to be made of the information and other relevant factors. Section 54(3) provides that in deciding the conditions on which information extracted from the Register, is to be given under this section, the Registrar must, as far as practicable, protect the persons to whom the entries in the Register relate from unjustified intrusion on their privacy. We have no knowledge as to whether the Registrar has decided that verifying documents via a DVS check represents an adequate reason for wanting the information extracted from the Register.

We consider that Victoria should consider whether a DVS request would fall within Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1998* (WA) and, if so, whether document verification through the DVS complies with s 54.

The Department of Transport - Driver and Vehicle Services is responsible for driver licences pursuant to the *Road Traffic Act 1974* (WA) and *Road Traffic (Authorisation to Drive) Regulations 2008* (WA). We do not consider that anything in the Act or Regulations is an impediment to the expansion of private sector access to the DVS. However, Western Australia may wish to give consideration to whether specific provision should be made for participation in the DVS.

14.3 Conclusion in respect of Western Australia

In summary, we consider that the expansion of private sector access to the DVS is legally permissible in Western Australia.

In our view, the Department of the Attorney General - Registry of Births, Deaths & Marriages should consider whether a DVS request would fall within Part 8, Division 4 of the *Births, Deaths and Marriages Registration Act 1998* (WA) and, if so, whether document verification through the DVS complies with s 54.

Schedule 1 - Glossary

AGD	The Commonwealth Attorney-General's Department
APP	Australian Privacy Principle
ATO	Australian Taxation Office
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Human Services
DVS Hub	The component of the DVS infrastructure that connects document issuing agencies and users/GSPs and allows for DVS match requests and responses to be securely routed between them
EOI	Evidence of Identity
FSM	Field Specific Matching, that is a response to a DVS query that indicates which of the fields did not match the records of the issuing agency
GSP/Gateway Service Provider	A Gateway Service Provider allows approved private sector and government users to interrogate the DVS through the Gateway Service Provider's interface. The GSP provides the channel through which users access the DVS or are authorised to access the DVS on behalf of a user who requires the identifying information to be matched
IPP	Information Privacy Principle
NPP	National Privacy Principle (now repealed)
OAIC	The Office of the Australian Information Commissioner
PIA	Privacy impact assessment
Privacy Act	The *Privacy Act 1988* (Cth) as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) with effect from 12 March 2014
User	A government agency or private sector organisation who uses the DVS to verify records against the issuing agency's records, either through direct access to the DVS through their own DVS interface or by using the services of a Gateway Service Provider

Schedule 2 - Documents considered in the course of the PIA

Background information

2. The information contained on the DVS website: www.dvs.gov.au

3. The information contained on the DVS page of the AGD website: http://www.ag.gov.au/rightsandprotections/identitysecurity/pages/documentverificationservice.aspx

4. *Document Verification Service: An Overview* (V4 December 2013)

5. *DVS Data Flow and Storage* flowchart

6. National Identity Security Coordination Group 23 November 2011 Item 4b

7. DVS Advisory Board 2 December 2013 Item 8

8. *Document Verification Service: Private Sector Access National Service Offering Industry Briefing Note* May 2013

Relevant policies

1. DVS Access Management policy: A policy for access to the Document Verification Service by Business Users

2. Document Verification Service An Overview for Private Sector Use V2.2 July 2013

Contractual documents

1. Document Verification Service: Gateway Service Provider Application Form and attached Document Verification Service Gateway Service Provider Terms and Conditions of Use

2. Document Verification Service: Business User Application Form and attached Document Verification Service Business User Terms and Conditions of Use

3. Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013

4. Document Verification Service Supporting Material - Module 3 Interface Definitions version 9 November 2013

5. Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013

Existing privacy impact assessments

6. Attorney-General's Department Cyber and Identity Security draft paper entitled Application of the APPs

7. Attorney-General's Department Privacy Impact Assessment: National Document Verification Service June 2007

8. Information Integrity Systems Draft Preliminary Privacy Assessment: Information Brokers Access to the Document Verification Service 17 July 2012

9. Information Integrity Systems Extension of Document Verification Service to Private Sector Organisations 20 July 2012

Document Verification Service - expanded private sector access, National Privacy Impact Assessment

Previous audits conducted by OAIC and its predecessor the Office of the Privacy Commissioner

1. National Document Verification Service, Department of Foreign Affairs and Trade, Department of Immigration and Citizenship, ACT Department of Births Deaths and Marriages, ACT Road User Services, Centrelink May 2009

2. National Document Verification Service, Department of Immigration and Citizenship - Audit Report March 2010

3. National Document Verification Service, Attorney-General's Department Final Audit Report May 2010

4. National Document Verification Service, Centrelink - Audit Report June 2011

5. National Document Verification Service - Department of Foreign Affairs and Trade - Audit Report December 2012

Schedule 3 - Contractual requirements

Defined terms in this Schedule are defined terms found in the Document Verification Service Business User Terms and Conditions of Use (**Attachment 2**) and Document Verification Service Gateway Service Provider Terms and Conditions of Use (**Attachment 3**).

1. DVS Business User Terms and Conditions of Use

Pursuant to the DVS Business User Terms and Conditions of Use (**Attachment 2**), a user must itself be an approved GSP or have in place an arrangement with a third party currently approved GSP: clause 2.2.

Users are required to strictly comply with all instructions and guidance provided by AGD: clause 7.

1.1 Secondary purpose

Except as may be specifically advised in writing by the AGD, users must not access or use the DVS for any purpose other than for the purposes of meeting statutory obligations in relation to identity verification (clause 8.1) and must not allow any person other than authorised personnel to access or use information match data or the DVS Business User ID (clause 8.3). Personal information obtained through use of the DVS must not be used for any purpose other than access to and use of the DVS: clause 8.5.

1.2 Privacy

Clause 11 of the DVS Business User Terms and Conditions of Use provides that "*You must ensure that your use of the DVS and Information Match Data complies with the Privacy Act 1988*".

Users must have a privacy policy (which must be attached to the Business User Application Form at **Attachment 3**), must comply with that policy and must not make any change to that policy without giving the AGD at least 30 days' notice in writing: clause 13.

1.3 Consent

DVS checks must be undertaken with the informed consent of the person whose information is being used. An individual providing their document details for verification must be "*informed of the purpose for which that information is sought and will be used by you (including that the information will be subject to an Information Match Request in relation to relevant Official Record Holder information, and that a corresponding Information Match Result will be provided via the use of third party systems*" (clause 12.2.) and must provide "*their express consent for such use and accessing such information prior to any such use or access being initiated or made by you*" (clause 12.3). However, users must not make any public statement concerning their access to the DVS or their use of the DVS: clause 8.6.

1.4 Auditing

Users and their GSPs must fully cooperate with any audit or verification process checking their compliance, including providing access to premises, facilities, systems and records: clause 10. DVS Information Match Responses must be recorded so that compliance with the Conditions can be audited: clause 2.4.

1.5 Security

Users must comply with all security procedures advised by the AGD and take all reasonable action to maintain the security of the DVS including maintaining the security of tokens, access codes, and encryption keys (clause 16) and must take all reasonable action to prevent and detect unauthorised use of the DVS or their Business Access Systems (clause 18). Users

must immediately notify the AGD of any suspected compromise of security information, unauthorised use or security breach (clause 18).

Users and GSPs can be suspended at any time for any reason (clause 24) and users can be terminated immediately for breach of the DVS Business User Terms and Conditions of Use (clause 25.2).

2. Gateway Service Provider Terms and Conditions of Use

2.1 Access

Pursuant to the Gateway Service Provider Terms and Conditions of Use (**Attachment 3**), GSPs cannot connect to the DVS and provide Gateway Services until the Gateway System has been fully tested and is compliant with the AGD's Gateway System certification requirements: clause 2.

GSPs are required to strictly comply with all instructions and guidance provided by the AGD: clause 10.

GSPs can only accept Authorised Business Users as Gateway Users who must be required to comply with the DVS Business User Terms and Conditions of Use: clauses 3 and 4. GSPs may not themselves make an Information Match Request unless they are also an Authorised Business User: clause 11.6.

GSPs must fully cooperate with any audit or verification process checking their compliance, including providing access to premises, facilities, systems and records: clause 13.

2.2 Security

GSPs must comply with all security procedures advised by the AGD and take all reasonable action to maintain the security of the DVS including maintaining the security of tokens, access codes, and encryption keys (clause 17) and must take all reasonable action to prevent and detect unauthorised use of the DVS or their Gateway Systems or Gateway Services (clause 18). Users must immediately notify the AGD of any suspected compromise of security information, unauthorised use or security breach (clause 19).

2.3 Privacy

GSPs must have a privacy policy (which must be attached the Gateway Services Agreement Form at **Attachment 3**), must comply with that policy and must not make any change to that policy without giving the AGD at least 30 days' notice in writing: subclauses 14.3 and 14.4.

Except as specifically authorised by the AGD in writing, GSPs must not collect or store Information Match Results: clause 11.5.

2.4 Consent

GSPs must ensure that the individual whose document details are being checked has provided his or her prior informed consent: clause 14.1.

3. DVS Supporting Materials

We understand that the instructions and guidance provided by the AGD (that GSPs must comply with pursuant to clause 10 of the Gateway Service Provider Terms and Conditions of Use, and users must comply with pursuant to clause 7 of the Business User Terms and Conditions of Use) currently include in the DVS Supporting Materials that are provided to GSPs.

The Supporting Materials provide that "*Access to the DVS will be for the sole purpose of confirming the integrity of identifying information provided by an individual as evidence of*

identity (EOI)": Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at section 4.5.

We note that the Document Verification Service *An Overview for Private Sector Use* V2.2 July 2013 provides that "*A positive or negative response received through the DVS may not be used as the sole basis for a decision to enrol or not enrol an individual for benefits or services*."

Users and GSPs are required to submit annual (or more frequent) compliance statements which must, at a minimum, confirm that the user's (or GSP's) use of the DVS is in accordance with the Terms and Conditions of Use and the DVS Supporting Material or, if the user did not fully comply with the Terms and Conditions of Use and DVS Supporting Material, what actions have been or are being taken to address the contravention: Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at sections 4.7 and 4.8.

GSPs are audited annually by independent auditors for compliance with the DVS terms and conditions (most users accessing the DVS through a GSP). GSPs either conduct the electronic search on behalf of the user or provide the customer identification service through which they are responsible for obtaining the details of the identity document and the individual's consent to the DVS check. Users are audited on the basis of risks identified in assessing compliance statements: Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at section 4.7.

3.1 **Security**

The DVS Supporting Materials with which users must comply include extensive security requirements: Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013; see also *Document Verification Service: An Overview* (V4 December 2013).

The DVS Hub allows requests and responses to be securely routed between users (or GSPs) and agencies. The DVS Hub has a number of security features including firewall and environment security, intelligent message transformation and routing and management information and audit logs.

DVS security policy is based on the Australian Government Protective Security Policy Framework (PSPF), the technology control minimum standards specified in the Australian Government Information Security Manual, and relevant Australian and New Zealand IT Security standards.

All user and GSP personnel who perform DVS ICT administrative or system functions must be employment screened in accordance with PSPF level 1 (government agencies) or with the Australian Standards AS4811:2006 – Employment Screening (private sector organisations).

Users and GSPs are required to log activity and transactional data to enable monitoring for and reporting of security breaches. Users, GSPs and issuing agencies are required to report security incidents or information security events to the DVS Operations Manager and the DVS Manager. Security incidents that must be reported include (but are not limited to):

- DVS targeted emails with attachments or links;
- any compromise or corruption of DVS information;
- unauthorised access or intrusion into a DVS ICT system;
- DVS data spills;
- introduction of viruses/malware to a network with DVS operations;

- theft or loss of electronic devices that have access to DVS systems or have processed or stored DVS data;
- evidence of attempted trawling ;
- Denial of Service attacks directed to DVS Internet based services; or
- suspicious or unauthorised network activity.

DVS Participants must have a designated Security Incident Investigator responsible for notifying the DVS Hub Security Incident Investigator and DVS Manager of any DVS security incidents. The DVS Hub Security Investigator will then report on the incident to the DVS Manager who will subsequently advise the National DVS Advisory Board: see Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013

Security incidents may also be reported to appropriate external parties (such as the police or the OAIC).

Attachment 1 - Invitation to comment

Document verification service

Consultation paper for national privacy impact assessments for proposals to enhance the document verification service

4 June 2014

If you have any questions about the details of this document
please contact Jan Cumming (+61 2 6279 4040)

Clayton Utz
Level 10 2 Phillip Law Street Canberra ACT 2601 Australia
GPO Box 9806 Canberra ACT 2601

REQUEST FOR ASSISTANCE FROM AGD

The Australian Government Attorney-General's Department (AGD) has commissioned Clayton Utz to prepare reports scoping the potential privacy impacts of proposals to enhance the availability and functionality of the national Document Verification Service (DVS) in terms of recent Commonwealth privacy reforms. The proposals involve both privacy risks and benefits in the context of each State and Territory's privacy regime, whether legislated or otherwise, and any other relevant State or Territory legislation. To develop the privacy impact assessments, AGD seeks your assistance in identifying these risks and benefits in the context of each State and Territory, as well as potential controls or mitigation strategies.

To this end, AGD has asked Clayton Utz to conduct targeted consultation with key stakeholders related to the national components of the service. This paper is intended to provide a brief overview of the proposals to assist in the consultation process.

The consultation process, and how you can assist, is set out in the next steps section of this paper (on page 5).

CONTENTS

Background—What is the DVS?

AGD manages the DVS on behalf of all Australian governments. The DVS is a key element of the National Identity Security Strategy endorsed by the Council of Australian Governments.

The DVS is a secure online system that enables organisations to verify information on a customer's evidence of identity documents with the records of the document issuing agency.

The DVS currently provides organisations with the ability to verify information on a range of evidence of identity documents issued by Australian Government and state and territory government agencies. These include immigration documents, passports, driver licenses, Medicare cards. Government agencies are also able to access birth, marriage, and change-of-name certificates.

The DVS is not a database. DVS transactions involve a check of whether the information presented on an evidence of identity document matches the records of the issuing agency. The results are provided in the form of a 'yes/no' result. DVS checks must be undertaken with the informed consent of the person whose information is being used, and no personal information is retained following the completion of a check.

DVS checks have been available to by government agencies since 2009, and are now being made available to the private sector, with an initial focus on organisations that have legislative obligations to identify their customers (for example, financial institutions which need to meet 'know your customer' requirements in anti-money laundering and counter-terrorism financing regulations).

Any organisation using the DVS is required to comply with the *Privacy Act 1988* (Cth) or any relevant State and Territory privacy legislation.

For further information on the DVS see www.dvs.gov.au.

Proposals to expand the functionality and availability of the DVS

AGD is considering two proposals which are set out below. In addition, some of the privacy risks and benefits which have already been identified are set out.

<table>
<tr><td rowspan="2">1</td><td>Expanded commercial access: Reforms to the Privacy Act 1988 which came into effect in March 2014 include amendments to the restrictions on the use by organisations of Commonwealth government identifiers (previously dealt with by NPP 7.2). The new Australian Privacy Principles (APP) 9.2 allows use of government identifiers by organisations in different circumstances, including where ‘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 activities or functions.’

The current DVS access management policy (see the Attachment at page 8) limits commercial access and use to businesses operating under legislated client identification requirements under Commonwealth legislation. This restriction was informed by the prohibitions and permissions of the previous NPPs (NPPs 7.2, 2.1). In light of privacy reforms AGD is reviewing DVS access policies and is considering in particular potential privacy risks in expanding the range of businesses eligible for DVS access as may be permitted under the APPs.</td></tr>
<tr><td>Potential privacy issues, risks and benefits:

• Defining the circumstances in which use of an identifier is "reasonably necessary" for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions
• Facilitating online transactions without the need for hardcopy identity documents to be provided
• Limiting use by organisations to circumstances only where there is a reasonable need to verify the identity of the individual for the organisation's activities or functions
• Avoiding more intrusive identity verification methods, for example avoiding the need for organisations to keep copies of identity documents</td></tr>
<tr><td>2</td><td>Expanded functionality (field specific matching): DVS technical functionality currently provides a one character response indicating the cumulative accuracy of all data fields used to match a document – a confirmed match (Y) response indicates that all five fields completely match. Negative responses provide no information as to why an N result is returned.

The challenge of translating the complexity of some identity documents into DVS match requests can result in inaccuracy at the data entry stage and the return of false ‘N’ responses. This can result in Users resubmitting queries</td></tr>
</table>

1	Expanded commercial access: Reforms to the Privacy Act 1988 which came into effect in March 2014 include amendments to the restrictions on the use by organisations of Commonwealth government identifiers (previously dealt with by NPP 7.2). The new Australian Privacy Principles (APP) 9.2 allows use of government identifiers by organisations in different circumstances, including where '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 activities or functions.' The current DVS access management policy (see the Attachment at page 8) limits commercial access and use to businesses operating under legislated client identification requirements under Commonwealth legislation. This restriction was informed by the prohibitions and permissions of the previous NPPs (NPPs 7.2, 2.1). In light of privacy reforms AGD is reviewing DVS access policies and is considering in particular potential privacy risks in expanding the range of businesses eligible for DVS access as may be permitted under the APPs.
	until a Y result is returned, generating multiple unnecessary N results and additional traffic through the system. Field specific matching (FSM) could assist Users to minimise the number of repeat match requests by providing a code from the Issuer indicating formatting errors or fields that were not matched in the search. Both public and private sector Users have indicated a strong interest in such a capacity. An FSM code would simply refer the User back to a specific field on the identity document for re-examination. AGD anticipates that FSM could deliver considerable service improvements to organisations and their customers by limiting the degree of guesswork in DVS requests, reducing the amount of retried queries, minimising the time taken to gain an accurate result, and improving customer service.
	Potential privacy risks and benefits: • Avoid unnecessary false negatives due to input error • Improve identity decision-making by providing Users with information to start a discussion with a customer • FSM could reduce the amount of information which is necessary for the purposes of verifying an identity • Whether there are other ways in which false negatives could be avoided without FSM

Privacy impact assessments into the proposals

AGD has instructed Clayton Utz to prepare two privacy impact assessments in relation to the two proposals discussed.

Report 1— Privacy impact assessment of expanded private sector access

We are instructed to prepare a Privacy Impact Assessment (PIA) identifying privacy impacts and options to mitigate any privacy risks related to extending use of the DVS to private sector organisations in the context of both the national privacy regime set out in the *Privacy Act 1988,* State and Territory privacy regimes, whether legislated or otherwise, and any other legislation relevant to the handling of information contained in evidence of identity documents issued by State or Territory agencies.

Report 1 will:

1) assess the privacy impacts (including risks and benefits) associated with expanding the range of organisations able to use the DVS for the purposes of verifying information on government issued identifiers to include any organisation with a 'reasonable necessity' to identify an individual as per Australian Privacy Principle (APP) 9.2(a), specifically as they relate to State and Territory privacy regimes, whether legislated or otherwise;

2) assess any privacy benefits that may accrue from wider private sector use of the DVS, as an alternative to other methods of verifying government issued identifiers that are commonly used by private sector organisations;

3) identify options to mitigate any privacy risks associated with expanded private sector use of the DVS; and

4) identify any provisions in legislation relevant to the handling of information contained in evidence of identity documents issued by State or Territory agencies, including road traffic and licensing legislation, that may impact on the proposed expansion of private sector to the DVS.

In doing so the report will need to take into account:

- previous Privacy Impact Assessments relating to the DVS
- the degree of privacy risks given broader legislative and quasi-legislative information privacy rules (e.g.. Existing privacy obligations under the *Privacy Act 1988* on business users)
- existing privacy and information security measures including contractual terms and conditions on DVS private sector access; existing privacy, information security, and business rules of the DVS, and
- governance processes for DVS private sector access.

Preparation of the report will include consultations with a range of Commonwealth, State and Territory government and non-government stakeholders such as:

- document issuing authorities – Department of Foreign Affairs and Trade, Department of Immigration and Border Protection, Department of Human Services, State and Territory Registries of Births, Deaths and Marriages and State and Territory driver licensing authorities;
- DVS User organisations – government and business;
- State and Territory Privacy and/or Information Commissioners, and
- Non-government privacy advocates

Report 2— Privacy Impact Assessment of Enhanced DVS Functionality (field specific responses)

We are instructed to prepare a Privacy Impact Assessment identifying privacy impacts and options to mitigate any privacy risks related to enhancing the DVS to return responses indicating the specific data field(s) that did or did not verify. The report will consider these impacts in the context of the proposed expansion of DVS private sector access (Report A).

Report 2 will:

1) assess the privacy risks associated with the enhanced DVS functionality providing data field specific responses,

2) assess the privacy benefits associated with enhanced DVS functionality, and

3) identify options to mitigate any privacy risks associated with the enhanced DVS functionality.

In doing so the report will need to take into account:

- the Privacy Impact Assessment of Expanded Private Sector Access
- existing privacy and information security measures including contractual terms and conditions on DVS private sector access, existing privacy, information security, and business rules of the DVS, and
- governance processes for DVS private sector access.

Preparation of the report will include consultations with a range of Commonwealth and State and Territory government and non-government stakeholders such as:

- document issuing authorities – Department of Foreign Affairs and Trade, Department of Immigration and Border Protection, Department of Human Services, State and Territory Registries of Births, Deaths and Marriages and State and Territory driver licensing authorities;
- DVS User organisations – government and business
- State and Territory Privacy and/or Information Commissioners, and
- Non-government privacy advocates

Next steps—how you can help

We have set out in the following section the questions which on which we would appreciate your thoughts. We are asking for written submissions by Wednesday 18 June 2014.

Questions for consultation

Generally:

- In addition to the DVS, what other methods (paper-based, electronic, etc) can organisations use to verify the identity of individuals?
- What might be the privacy impacts of those other identity verification processes (document copying, record keeping, etc)?
- Taking into account the existing controls on DVS access, what do you consider to be the current level of privacy risk associated with DVS use by government agencies and other eligible organisations?
- • Can you identify any potential scenarios in which these risks might materialise?

In relation to each proposal:

- What impact does your State or Territory's privacy regime have on the lawfulness of the proposal?
- What impact does your State or Territory's laws relating to the handling of information on evidence of identity documents (such as driver licences, birth certificates and marriage certificates) have on the lawfulness of the proposal?
- In what circumstances could the proposal have a positive privacy impact for individuals whose identities are being verified by an organisation?
- In what circumstances could the proposal have a negative privacy impact for individuals whose identities are being verified by an organisation?
- In what ways could any negative privacy impacts be managed?
- What additional security or access controls should be adopted if the proposal is adopted?
- What information should individuals be given about DVS transactions if the proposal is adopted?

In relation to the expanded private sector access proposal:

- What identity verification obligations or authorities currently apply to private sector organisations in your State or Territory under either:
  - State and Territory legislation; or
  - other non-legislative arrangements managed by State or Territory government agencies?

In relation to the field specific responses proposal:

- Can you identity any potential alternative approaches for improving the accuracy of data entry as part of requests for DVS checks that also take account of privacy impacts?

Please also address any other issues you see with the proposals.

Attachment— Policy for access to the Document Verification Service by Business Users

The nationally agreed policy for the commercial DVS limits its use to businesses with legislated identification obligations. In consultation with national stakeholders, AGD is exploring the potential for expanded private sector use, initially as it might align with the recent reforms to the Commonwealth privacy regime.

Access policy context

In the first phase of extending access to DVS to the private sector, it will be provided to entities that have a client identification requirements under Commonwealth legislation. Government already regulates the operations of these agencies. Access to the DVS will take account of these existing risk-based regulatory procedures. Given all governments' stated objective is to reduce red tape for industry, DVS represents a method that can potentially streamline and reduce these regulatory burdens, rather than creating new procedures. Examples of regulatory authorities that oversee likely DVS users are:

- ACMA
- Austrac
- APRA
- Office of Transport Security
- OAIC (including the Privacy Commissioner)
- ASIC

Business Users must also be subject to the privacy regime set out under the National Privacy Principles and the Privacy Act 1988.

Principles for access

The DVS is a commercial service and will operate on commercial lines. DVS Business User Applications will be accepted on a 'first-come, first-served' basis. Private sector organisations applying to become an approved DVS Business User need to meet the following requirements:

1. are subject to the Privacy Act 1988,
2. have a demonstrable requirement under law to verify the identity of their clients
3. are employing the DVS for an appropriate use, e.g. client registrations
4. operate within a regulatory regime, e.g. a banking or financial service licencing schemes in the case of financial institutions.
5. will agree to comply with all DVS private sector requirements, e.g. obtaining the informed consent of their clients, ICT and information security controls, logging and monitoring use, compliance reporting and audits etc. , and
6. will agree to undergo independent audits of their use of the DVS

Where the DVS Advisory Board does not have a specific and material objection to the organisation and the organisation pays the applicable fees at the time of application, it will be approved as a DVS Business User.

Attachment 2 - Document Verification Service Business User Terms and Conditions of Use

Document Verification Service
BUSINESS USER APPLICATION FORM

This Application is made by:

Applicant Business *(*full legal entity name):			
A.C.N	A.B.N.	Other relevant registration details (if any)	
Physical Address:			Postcode:
Postal Address:			Postcode:

Applicant Business Type: (check one only)

- ☐ *cash dealer* (as defined in the *Financial Transaction Reports Act 1988* and the *Financial Transaction Reports Regulations 1990*)
  State relevant type/s of service:
- ☐ Provider of a designated service (*reporting entity* as defined in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*)
  State type/s of designated service:
- ☐ superannuation service provider (regulated parties i.e. *trustee, superannuation entity* under the *Superannuation Industry (Supervision) Act 1993,* the *Superannuation Industry (Supervision) Regulations 1994*, the *Retirement Savings Account Act 1997* and the *Retirement Savings Accounts Regulations 1997*)
  State type/s of service:
- ☐ telecommunications service provider (*carriage service providers* or *mobile virtual network operator* under the *Telecommunications Act 1997*
  State type/s of service:
- ☐ credit report provider to which applies the Credit Reporting Code of Conduct made under the Privacy Act 1988
  State type/s of service:
- ☐ Other (please describe):
  State type/s of service:

Applicant Authorised Representative:		
Name:	Position:	
Telephone:	Fax:	Email:
Nominated Gateway Service Provider *(where relevant)***:**		
Name:	Position:	
Telephone:	Fax:	Email:

Applicant Privacy Policy : Please attach a copy of your privacy policy that will be applicable to your Gateway Service ☐ **CONFIRM ATTACHED**
by ticking the box

to:

Commonwealth of Australia represented by the **Attorney-General's Department**, A.B.N. **92 661 124 436** ('AGD') and each Official Record Holder.

Australian Government
Attorney-General's Department

Document Verification Service
BUSINESS USER APPLICATION FORM

1. The Applicant hereby applies to AGD to be provided with access to the Document Verification Service in accordance with the Document Verification Service Business User Terms and Conditions of Use.

2. The Applicant represents and warrants that all information provided in respect to this Application is true, correct, accurate and not misleading.

3. The Applicant acknowledges and agrees that, should AGD approve this Application, in consideration for that approval the Applicant has agreed to and will be legally bound by and must observe the Document Verification Service Terms and Conditions of Use (which the applicant acknowledges that it has received, read and understood prior to making this Application) as and from the date AGD advises the Applicant in writing that its Application has been approved.

4. The Applicant further acknowledges and agrees that in consideration of Austroads agreeing with AGD to provide Information Match Results in relation to driver license information in connection with the Document Verification Service and to perform other obligations to AGD, as and from the time the Applicant first issues an Information Match Request in respect of a drivers' licence Supported Document it will be legally bound by and must observe the Document Verification Service Terms and Conditions of Use under an additional and separate contract with Austroads.

Signed for and on behalf of the Applicant by

_____

Signature of Applicant's duly authorised representative

_____

Full name of Applicant's duly authorised representative

_____

Title of Applicant's duly authorised representative

Date / /

Australian Government
Attorney-General's Department

Document Verification Service Business User
TERMS AND CONDITIONS OF USE

Introduction

1 Your access to and use of the DVS is subject to these Document Verification Service Business User Terms and Conditions of Use (these Conditions).

Pre-conditions to DVS use

2 To be able to connect to the DVS you must:

2.1 have an operational DVS Business User ID;

2.2 either yourself be an current Approved Gateway Service Provider or have in place an arrangement with a third party current Approved Gateway Service Provider

2.3 ensure any DVS Information Match Results you receive are recorded so as to allow us to efficiently and effectively audit your compliance with these Conditions

2.4 meet all other requirements we may advise you of to enable you to access and use the DVS.

Use

3 You must ensure that all relevant members of your Personnel are aware of and comply with these Conditions.

4 You must ensure that your use of the DVS does not (and does not attempt to) modify, interfere with, disrupt, adversely affect or misuse the DVS or DVS functionality in any way, or interfere with or disrupt use of the DVS by any other person.

5 You must ensure that your use of the DVS and Information Match Data complies with all laws, regulatory requirements, and complies with all codes of conduct to which you ascribe.

6 You must promptly provide us with any information we request in respect to your access to or use of the DVS, including any routine reports and certifications.

7 You must strictly comply with all instructions and guidance we advise to you in respect to your access to and use of the DVS and Information Match Results and any other related matter.

8 Except as may be specifically authorised by us in writing, you must:

8.1 only access and use the DVS and Information Match Data to assist you in meeting your statutory obligations in relation to identity verification

8.2 not allow any person other than your authorised Personnel to access or use Information Match Data or your DVS Business User ID

8.3 only access and use the DVS and Information Match Data exclusively for your own internal purposes

8.4 not collect, store or use Information Match Results for any purpose associated with the provision, or potential provision of, an information service to any person

8.5 not use or disclose any personal information (as defined in the *Privacy Act 1988* (Cth)) obtained through your use of the DVS for any purpose other than your access and use of the DVS

8.6 not make any public statement concerning the DVS or your access to or use of it .

9 You must not, by act or omission, directly or indirectly, mislead any person in relation to the DVS, your access to or use of the DVS or any related matter.

10 You and your Approved Gateway Service Provider must fully cooperate with and support any audit or verification process we (or our agents) wish to conduct to verify your compliance with these Conditions, without limitation including providing us with prompt access to relevant records, systems, premises and facilities. You authorise us to have access to any records or information held by any Approved Gateway Service Provider relevant to your access to or use of the DVS.

Privacy, consent and information use

11 You must ensure that your use of the DVS and Information Match Data complies with the *Privacy Act 1988.*

12 You must ensure that each individual providing details in a Supported Document to you:

12.1 confirms they are authorised to provide those details to you

12.2 is informed of the purpose for which that information is sought and will be used by you (including that the information will be subject to an Information Match Request in relation to relevant Official Record Holder information, and that a corresponding Information Match Result will be provided via the use of third party systems)

12.3 provides you with their express consent for such use and accessing such information prior to any such use or access being initiated or made by you

and that you keep full and proper records of all such disclosures, confirmations and consents.

13 You must:

13.1 comply with your own privacy policy

13.2 not make any change to your privacy policy without notifying us of the change, and where possible give us no less than 30 days day prior written notice of any proposed change.

Your facilities

14 You must provide everything that you need to access and use the DVS and ensure that your equipment and facilities are properly configured and otherwise meets all relevant requirements advised by us.

Fees and charges

15 You must pay all fees and charges advised to you in respect to you being a DVS Business User. Unless specifically stated to the contrary, all fees, once incurred are payable and once paid are non-refundable, including where your access to or use of the DVS is cancelled, suspended or terminated for any reason.

Security

16 You must comply with all security procedures advised to you in relation the DVS and take all reasonable action to protect and maintain the security of the DVS and your access to and use of it, including, without limitation, maintaining the security of all tokens, access codes, encryption keys and other information relating to access, authentication or security relating to the DVS.

17 You must take all reasonable action to prevent and detect unauthorised use of the DVS and your Business Access System.

18 You must immediately notify us if you know or suspect that access or authentication security information has been compromised or any other kind of unauthorised use or security breach has occurred, or if you know or suspect that there is a security vulnerability, fault, error or problem in the DVS or any Information Match Result.

Updates and changes to the DVS

19 The DVS may be upgraded and its features, functionality and other characteristics may change from time to time. We will endeavour to provide reasonable notice of any changes that we consider are not routine and should be advised to DVS Business Users. You acknowledge that it may not be reasonably possible to provide notice in all circumstances and that in no event will we be obliged to provide notice exceeding 14 days.

The DVS is provided 'as is' and 'as available'

20 The DVS has been implemented in a technical environment that is designed to provide high availability and be fault tolerant. However, as with any technology based facility, the speed and characteristics of the DVS will vary at different times and under different circumstances and the DVS may not always work as described, and the DVS and Information Match Results may be subject to faults, errors, interruption or breakdown or be fully or partially unavailable. You acknowledge and agree that, subject to clause 92, your access to and use of the DVS is on an 'as is, as available' basis only, and without limiting the foregoing:

20.1 you must ensure your business processes and operations can be satisfactorily conducted despite the DVS or Information Match Results being subject to faults, errors, interruption or breakdown or be fully or partially unavailable for any reason

20.2 any information we provide regarding availability, performance or other service levels or characteristics relating to the DVS, no matter how expressed, are non-contractual statements of intent only and do not constitute a representation or warranty of any kind.

21 You acknowledge and agree that you:

21.1 are solely responsible for your business processes and decisions

21.2 must, where any issues arise with your customers or other stakeholders that in any way relate to your access to or use of the DVS or Information Match Data, ensure that the relevant customers and stakeholders understand that you are the sole point of contact in relation to those issues

21.3 must manage and resolve all such issues yourself as expeditiously as possible and without seeking to involve us or in any way

Changes to these Conditions

22 We can update or otherwise vary these Conditions by not less than 45 days prior written notice to you.

Cancellation

23 We will promptly cancel your DVS Business User ID if you notify us to do so. We will advise you once cancellation has been effected.

Suspension and Termination

24 We may refuse access to the DVS, or suspend its operation in whole or in part either for you as a specific DVS Business User, for any Approved Gateway Service Provider or generally, at any time for any reason we think fit.

25 We may terminate you DVS Business User ID:

25.1 with or without cause at any time by not less than 45 days prior written notice to you

25.2 where you have breached these Conditions, immediately by written notice to you.

Indemnity

26 Subject to clause 92, you indemnify us against any loss, damage, cost, expense (including legal expenses on a solicitor and own client basis), claim, proceeding or liability of any kind that we (or our Personnel) may incur, that arises (no matter how arising including from negligence by us) out of or in connection with, your use (including unauthorised use) of your DVS Business User ID, your access to or use of the DVS, the correctness or otherwise of Information Match Results, your Gateway Service or the lawful exercise of our rights pursuant to these Conditions.

Priority

27 To the extent of any inconsistency between a provision in this document and any other provision forming part of these Conditions, the provision in this document will prevail.

Disclaimer and liability

28 You acknowledge that we provide Information Match Results based on information which may be provided to us by third parties and that where that is the case we have not independently verified the accuracy or completeness of information provided by those third parties. Subject to clause 92, the DVS and Information Match Results are made available without any representation or warranty of any kind (without limitation in respect to the accuracy of Information Match Results) and we have no liability to you in respect of any loss or damage that you might suffer no matter how arising (including from negligence by us) that is directly or indirectly related to the DVS, or Information Match Results or any other relevant matter, without limitation including any Gateway Service and, any Approved Gateway Service Provider.

29 Except as set out in this clause 92, nothing in these Conditions excludes, restricts or modifies the application of, or liability in respect of, any consumer guarantee that applies to these Conditions under the Australian Consumer Law (Consumer Guarantee). Our liability for any failure by us to comply with a Consumer Guarantee that applies to these Conditions is limited to us (at our election):

29.1 supplying the services again; or

29.2 paying the cost of having the services supplied again,

except where it is not 'fair or reasonable' (as contemplated under section 64A of the Australian Consumer Law) for us to do so.

Notice

30 We may advise or notify you of any matter in relation to the DVS and these Conditions by email, mail, facsimile or telephone to any relevant address or number that you have provided to us.

Definitions

31 In these Conditions, unless the context implies a contrary intention, the following terms have the meaning set out below:

Approved Gateway Service Provider means a provider of a Gateway Service that is at all relevant times approved by us.

Australian Consumer Law means Schedule 2 to the *Competition and Consumer Act* 2010 (Cth) and the corresponding provisions of the Australian Consumer Law (ACT) or any other state or territory as applicable.

Austroads means Austroads Ltd ACN 136 812 390.

Business Access System means systems and facilities that you use to connect to and interact with the DVS.

DVS means the system (including all associated services, infrastructure, applications, facilities, functionality, data, information and material, whether belonging to or operated by us or a third party) established by us to provide Information Match Results (but does not include any Gateway Service).

DVS Business User ID means a number or other mechanism (and associated access credentials) provided by us by which you are uniquely identified to us for purposes including accessing the DVS, transaction processing, and record keeping.

DVS Testing Environment means any system or facility we make available to you for testing purposes.

Gateway Service means the services and facilities (forming part of your Business Access System) by which your internal systems connect to the DVS.

Information Match Data means data and information in or relating to Information Match Requests or Information Match Results.

Information Match Request means an electronic request to the DVS by a User (required to be submitted in a structured electronic format advised by us) to be provided with an Information Match Result in relation to the details of relevant information in a Supported Document.

Information Match Result means, in respect to an Information Match Request, an electronic response indicating that the information provided in the request either matches or does not match the relevant official record data, or that a system error has been encountered in trying to process that request.

Official Record Holder means, in respect of each Supported Document, the entity against whose official record data the information submitted in an Information Match Request is matched (or attempted to be matched) via the DVS.

Personnel includes employees, officers, directors, contractor and agents.

Supported Document means a type of document (for example an Australian Passport or Australian Citizenship Certificate) that is supported by the Document Verification Service.

User means each person (and, if relevant, each automated system) who can initiate an Information Match Request in relation to your DVS Business User ID.

we and **us** means Commonwealth of Australia acting represented by the Attorney-General's Department and, in relation to clauses 83, 89, 91 and 92, also includes each Official Record Holder and (in the case of driver's licence information) Austroads.

you means the relevant DVS Business User, and, as the context admits, each relevant User.

Australian Government
Attorney-General's Department

Document Verification Service Business User
Addendum 1 – Fee Schedule

Business User Application Fee

As an originator of verification requests *Business Users* will need to be approved by the DVS Advisory Board and sign a formal application. A *Business User* that seeks to use the DVS will be charged a $5,000 **application fee,** if it submits this form unamended, to cover the cost of assessing and approving applications.

Connection Fee

Businesses which establish **a direct ICT connection to the DVS** will be acting as *Gateway Service Providers* (GSPs). They may be accessing the DVS on their own behalf as an approve Business User, or in order to provide services to other *Business User* clients. GSPs will be charged $50,000 to link their systems to the DVS Hub infrastructure via Web Services, including test and 'sandpit' environments, testing processes and migration into the production environment. The connection fee includes an amount payable to current DVS IT service providers together with AGD's internal costs. The price of a non-Web Services connection will be advised on a case-by-case basis.

Transaction Fees

A tiered schedule of transaction fees is **payable by the party connecting directly to the DVS** (i.e. GSP) which will vary based on the volume of transactions. Where a GSP's annual Information Match Requests number 400,000 or less, a fee of $1.40 is proposed for each and every Request that does not encounter a DVS system error Match Result. The transaction fee progressively falls to $0.65 once the GSP's annual volume exceeds 1 million transactions per annum.

Annual Volume	per calendar month	per query charge
< 400,000	<33,000	$1.40
>400,001 <600,000	>33,000 <50,000	$1.20
>600,001 <800,000	>50,000 <65,000	$1.00
>800,001 <1 million	>65,000 <85,000	$0.80
>1 million	>85,000	$0.65

Pricing Issues

GST

GST will be levied on DVS costs.

Review

DVS prices will be reviewed annually and may decrease.

Australian Government
Attorney-General's Department

Document Verification Service Business User

Addendum 2 – Document availability by Type and Jurisdiction

Australian Driver Licences	New South Wales
	Victoria
	Queensland
	Western Australia
	South Australia
	Tasmania
	Australian Capital Territory
	Northern Territory
Medicare Cards	Australian Resident (Green)
	Interim Card (Blue)
	Reciprocal Health Care Agreement (Yellow)
Australian Travel Documents	Passport (including Ordinary, Frequent traveller, Diplomatic, Official and Emergency)
	Certificate of Identity
	Document of Identity
	UN Convention Travel Document
Australian Visas	Not including: Some Bridging Visas and Humanitarian Visas or PLO56
Citizenship Certificates	
Registration by Descent Certificates	
Irregular Maritime Arrival Cards	Evidence of Immigration Status (EIS) ImmiCard (Pink)
	Permanent Residence Evidence (PRE) ImmiCard (Green)

Attachment 3 - Document Verification Service Gateway Service Provider Terms and Conditions of Use

Australian Government
Attorney-General's Department

Document Verification Service
GATEWAY SERVICE PROVIDER AGREEMENT FORM

This application is made by:

Applicant *(*full legal entity name):			
A.C.N	A.B.N.	Other relevant registration details (if any)	
Physical Address:			Postcode:
Postal Address:			Postcode:
Applicant Authorised Representative Name: Position:			
Telephone:	Fax:	Email:	
Applicant Privacy Policy : Please attach a copy of your privacy policy that will be applicable to your Gateway Service ☐ **CONFIRM ATTACHED** by ticking the box			

to:

Commonwealth of Australia represented by the **Attorney-General's Department**, A.B.N. **92 661 124 436** ('AGD') and each Official Record Holder.

1. The Applicant hereby applies to AGD to be approved as a Document Verification Service Gateway Service Provider.

2. The Applicant represents and warrants that all information provided in respect to this Application is true, correct, accurate and not misleading.

3. The Applicant acknowledges and agrees that, should AGD approve this Application, in consideration for that approval the Applicant has agreed to and will be legally bound by and must observe the Document Verification Service Gateway Service Provider Terms and Conditions of Use (which the applicant acknowledges that it has received, read and understood prior to making this Application) as and from the date AGD advises the Applicant in writing that its application has been approved.

4. The Applicant further acknowledges and agrees that in consideration of Austroads agreeing with AGD to provide Information Match Results in relation to driver license information in connection with the Document Verification Service and to perform other obligations to AGD, as and from the time the Applicant first issues an Information Match Request in respect of a drivers' licence Supported Document it will be legally bound by and must observe the Document Verification Service Gateway Service Provider Terms and Conditions of Use under an additional and separate contract with Austroads.

Signed for and on behalf of the Applicant by

_____

Signature of Applicant's duly authorised representative

_____

Full name of Applicant's duly authorised representative

_____

Title of Applicant's duly authorised representative

Date / /

Australian Government

Attorney-General's Department

Document Verification Service Gateway Service Provider TERMS AND CONDITIONS OF USE

Introduction

32 Your access to and use of the DVS is subject to these Document Verification Service Gateway Service Provider Terms and Conditions of Use (these Conditions).

Pre-conditions to DVS access

33 To be able to connect to the DVS and provide Gateway Services you must:

- 33.1 have an operational DVS Gateway Service Provider Account;
- 33.2 have a Gateway System that meets all requirements we have advised to you;
- 33.3 ensure your Gateway System has been thoroughly tested:
  - (a) within your own environment
  - (b) within the DVS Testing Environment (unless otherwise agreed in writing by us) and
  - (c) with each of your Gateway Users.
- 33.4 ensure you have complied with any Gateway System certification requirements advised by us
- 33.5 ensure your Gateway System includes a process that ensures each of your Gateway Users is properly authenticated and that the Gateway System (and other relevant systems) maintain comprehensive records of each Gateway User's use of the Gateway System and its access to and use of the DVS generally so as to allow us to efficiently and effectively audit your compliance with these Conditions
- 33.6 have obtained written confirmation from us that we have registered the relevant IP address(es) that you will use in respect to your access to and use of the DVS
- 33.7 meet all other requirements we may advise you of to enable you to access and use the DVS.

Use

34 Before accepting anyone as a Gateway User, you must ensure that they are an Authorised Business User.

35 Your contractual arrangements with Gateway Users must require you to comply with the Document Verification Service Business User Terms and Conditions of Use.

36 You must provide reasonable assistance to prospective Gateway Users to ensure they can become Authorised Business User as quickly and conveniently as possible.

37 You must ensure that all your Personnel are aware of and comply with all provisions of these Conditions that are relevant to their role, function and duties.

38 You must ensure that your Gateway System, your Gateway Services and your Gateway Users do not (and do not attempt to) modify, interfere with, disrupt, adversely affect or misuse the DVS or DVS functionality in any way, or interfere with or disrupt use of the DVS by any other person.

39 You must ensure that your (and take all reasonable steps to ensure that Gateway Users') access to and use of the DVS is properly authorised, complies with all laws, regulatory requirements, and complies with all codes of conduct to which you ascribe.

40 You must promptly provide us with any information we request in respect to your access to your Gateway System, Gateway Services and use of the DVS, including any routine reports and certifications.

41 You must strictly comply with all instructions and guidance we advise to you in respect to your Gateway System, your access to and use of the DVS and Information Match Results and any other related matter.

42 Except as may be specifically authorised by us in writing, you must:

- 42.1 not allow any person other than your authorised Gateway Users to use your Gateway Service
- 42.2 only access and use the DVS to provide your Gateway Service and for no other purpose
- 42.3 not outsource or externally host any aspect of your Gateway System or Gateway Service
- 42.4 not collect or store Information Match Results
- 42.5 not collect, store or use Information Match data for any purpose other than is strictly necessary to provide the Gateway Serviced directly to the requesting Gateway User
- 42.6 not yourself make any Information Match Requests (other than if you are also an Authorised Business User and make such requests in that capacity as Gateway User)
- 42.7 not make any public statement concerning the DVS or your access to or use of it .

43 You must not, by act or omission, directly or indirectly, mislead any person in relation to the DVS, your access to or use of the DVS, your Gateway Service, your Gateway System or any related matter.

44 You must fully cooperate with and support any audit or verification process we (or our agents) wish to conduct to verify your compliance with these Conditions, or your Gateway Users' compliance with all their obligations relating to the DVS, without limitation including providing us with prompt access to relevant records, systems, premises and facilities and ensuring you have any necessary consents from any person to do so.

Privacy, consent and information use

45 You must:

- 45.1 ensure that the data subject of each Information Match Request has provided his or her prior express consent to the provision, access and use of all personal information relevant to them that is necessary for you to provide your Gateway Service and for us to provide the DVS
- 45.2 not use or disclose any information obtained from us or your Gateway Users for any purpose other than is strictly necessary for you to provide your Gateway Service and to comply with these Conditions
- 45.3 in addition to any other requirement, strictly comply with your own privacy policy relevant to your

Gateway Service

45.4 not make any change to your privacy policy relevant to your Gateway Service without notifying us of the change, and where possible give us not less than 30 days day prior written notice of any proposed change.

Your facilities

46 You must provide everything that you need to provide your Gateway System and Gateway Service and to access and use the DVS and ensure that your equipment and facilities are properly configured and otherwise meets all relevant requirements advised by us.

Fees and charges

47 You must pay all fees and charges advised to you in respect to the use of your DVS Gateway Service Provider Account and your access to the DVS.

Security

48 You must comply with all security procedures advised to you in relation to the DVS and take all reasonable action to protect and maintain the security of the DVS and your access to and use of it, including, without limitation, maintaining the security of all tokens, access codes, encryption keys and other information relating to access, authentication or security relating to the DVS.

49 You must take all reasonable action to prevent and detect unauthorised use of the DVS and your Gateway System and Gateway Services.

50 You must immediately notify us if you know or suspect that access or authentication security information has been compromised or any other kind of unauthorised use or security breach has occurred in respect to the DVS, your Gateway System, Gateway Service or Gateway Users, or if you know or suspect that there is a security vulnerability, fault, error or problem in the DVS, any Information Match Result, or your Gateway System, Gateway Service or Gateway Users' systems.

Updates and changes to the DVS

51 The DVS may be upgraded and its features, functionality and other characteristics may change from time to time. We will endeavour to provide reasonable notice of any changes that we consider are not routine and should be advised to users. You acknowledge that it may not be reasonably possible to provide notice in all circumstances and that in no event will we be obliged to provide notice exceeding 14 days.

The DVS is provided 'as is' and 'as available'

52 The DVS has been implemented in a technical environment that is designed to provide high availability and be fault tolerant. However, as with any technology based facility, the speed and characteristics of the DVS will vary at different times and under different circumstances and the DVS may not always work as described, and the DVS and Information Match Results may be subject to faults, errors, interruption or breakdown or be fully or partially unavailable. You acknowledge and agree that, subject to clause 92, your access to and use of the DVS is on an ‘as is, as available’ basis only, and without limiting the foregoing:

52.1 you must ensure your business processes and operations can be satisfactorily conducted despite the DVS or Information Match Results being subject to faults, errors, interruption or breakdown or be fully or partially unavailable for any reason

52.2 any information we provide regarding availability, performance or other service levels or characteristics relating to the DVS, no matter how expressed, are non-contractual statements of intent only and do not constitute a representation or warranty of any kind.

53 You acknowledge and agree that you:

53.1 are solely responsible for your business processes and decisions

53.2 you are fully responsible for all access to and use of the DVS made via your Gateway System and Gateway Services, including use by your Gateway Users and any unauthorised use (both of which constitute your use for the purposes of these Conditions).

53.3 must, where any issues arise with your Gateway Users or other person that in any way relates to your Gateway System, Gateway Services or access to or use of the DVS, ensure that they understand that you are the sole point of contact in relation to those issues

53.4 must manage and resolve all such issues yourself as expeditiously as possible and without seeking to involve us in any way.

Changes to these Conditions

54 We can update or otherwise vary these Conditions by not less than 45 days prior written notice to you.

Cancellation

55 We will promptly cancel your DVS Gateway Service Provider Account and your access to the DVS if you notify us to do so. We will advise you once cancellation has been effected.

Suspension and Termination

56 We may refuse access to the DVS, or suspend its operation in whole or in part either for you as a specific Gateway Service Provider, or for any or all of your Gateway Users or generally, at any time for any reason we think fit.

57 We may terminate your access to the DVS or your DVS Gateway Service Provider Account:

57.1 with or without cause at any time by not less than 45 days prior written notice to you

57.2 where you have breached these Conditions, immediately by written notice to you.

Indemnity

58 Subject to clause 30, you indemnify us against any loss, damage, cost, expense (including legal expenses on a solicitor and own client basis), claim, proceeding or liability of any kind that we (or our Personnel) may incur, that arises (no matter how arising including negligence by us) out of or in connection with, your use (including unauthorised use) of your DVS Gateway Service Provider Account, your access to or use of the DVS, the correctness or otherwise of Information Match Results, your Gateway System, your Gateway Service, your Gateway Users or the lawful exercise of our rights pursuant to these Conditions.

Priority

59 To the extent of any inconsistency between a provision in this document and any other provision forming part of

these Conditions, the provision in this document will prevail.

Disclaimer and liability

60 You acknowledge that we provide Information Match Results based on information which may be provided to us by third parties and that where that is the case we have not independently verified the accuracy or completeness of information provided by those third parties. Subject to clause 30, the DVS and Information Match Results are made available without any representation or warranty of any kind (without limitation in respect to the accuracy of Information Match Results) and we have no liability to you in respect of any loss or damage that you might suffer no matter how arising (including from negligence by us) that is directly or indirectly related to the DVS, or Information Match Results or any other relevant matter, without limitation including any Gateway Service and, any Approved Gateway Service Provider.

61 Except as set out in this clause 30, nothing in these Conditions excludes, restricts or modifies the application of, or liability in respect of, any consumer guarantee that applies to these Conditions under the Australian Consumer Law (Consumer Guarantee). Our liability for any failure by us to comply with a Consumer Guarantee that applies to these Conditions is limited to us (at our election):

61.1 supplying the services again; or

61.2 paying the cost of having the services supplied again,

except where it is not 'fair or reasonable' (as contemplated under section 64A of the Australian Consumer Law) for us to do so.

Notice

62 We may advise or notify you of any matter in relation to the DVS and these Conditions by email, mail, facsimile or telephone to any relevant address or number that you have provided to us.

Definitions

63 In these Conditions, unless the context implies a contrary intention, the following terms have the meaning set out below:

Australian Consumer Law means Schedule 2 to the *Competition and Consumer Act* 2010 (Cth) and the corresponding provisions of the Australian Consumer Law (ACT) or any other state or territory as applicable.

Austroads means Austroads Ltd CAN 136 812 390

Authorised Business User means a legal entity that is (at the relevant point in time) authorised by us to issue Information Match Requests to and receive Information Match results from the DVS.

Document Verification Service Business User Terms and Conditions of Use means at any point in time the then current the terms and conditions published by AGD under which access to and use of the DVS is made available to Authorised Business Users.

DVS means the system (including all associated services, infrastructure, applications, facilities, functionality, data, information and material, whether belonging to or operated by us or a third party) established by us to provide Information Match Results (but does not include any Gateway Service).

DVS Gateway Service Provider Account means an account (and associated access credentials) by which you are uniquely identified to us for purposes including accessing the DVS, transaction processing, record keeping and billing.

DVS Testing Environment means any system or facility we make available to you for testing purposes.

Gateway Service means a service that enables Authorised Business Users to connect to and interact with the DVS.

Gateway System means systems and facilities that you use to provide a Gateway Service.

Gateway User means an Authorised Business User to who you are providing a Gateway Service.

Information Match Data means data and information in or relating to Information Match Requests or Information Match Results (other than information required to be kept in accordance with clause 96.5).

Information Match Request means an electronic request to the DVS by an Authorised Business User (required to be submitted in a structured electronic format advised by us) to be provided with an Information Match Result in relation to the details of relevant information in a Supported Document.

Information Match Result means, in respect to an Information Match Request, an electronic response indicating that the information provided in the request either matches or does not match the relevant official record data, or that a system error has been encountered in trying to process that request.

Official Record Holder means, in respect of each Supported Document, the entity against whose official record data the information submitted in an Information Match Request is matched (or attempted to be matched) via the DVS.

person includes a natural person, partnership, unincorporated or incorporated association, corporation or body politic.

personal information has the meaning defined in the *Privacy Act 1988* (Cth)

Personnel includes employees, directors, officers, agents and contractors.

Supported Document means a type of document (for example an Australian Passport or Australian Citizenship Certificate) that is supported by the Document Verification Service.

we and **us** means Commonwealth of Australia acting represented by the Attorney-General's Department and, in relation to clauses 83, 89, 91 and 92 also includes each Official Record Holder and (in the case of driver's licence information) Austroads.

you means the relevant DVS Gateway Service Provider Account holder, and, as the context admits, each relevant member of your Personnel

CLAYTON UTZ

Document Verification Service

Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS

15 May 2014

Clayton Utz
Lawyers
Level 10, NewActon Nishi
2 Phillip Law Street
Canberra ACT 2601
GPO Box 9806
Canberra ACT 2601
Tel +61 2 6279 4000
Fax +61 2 6279 4099
www.claytonutz.com

Our reference 213/15921/80151527

Contents

1. Introduction and outline

The Document Verification Service (or in this document, the **DVS**) is a secure online system that enables organisations to verify information on documents issued by Australian Government and state and territory government agencies (in this document, **evidence of identity documents**) as against the records of the document issuing agency. The evidence of identity documents include immigration documents, passports, driver licenses, Medicare cards and birth certificates.

The DVS is currently available to government agencies and is being made available to private sector organisations that have Commonwealth legislative obligations to identify their customers (such as under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)).

DVS transactions currently involve a check of whether the information presented on an evidence of identity document matches the records of the issuing agency. The results are currently provided in the form of a 'yes/no' result.

The reforms to the *Privacy Act 1988* (Cth) (**Privacy Act**) with effect from 12 March 2014 include amendments to the use by organisations of government related identifiers (previously dealt with by National Privacy Principle (**NPP**) 7.2). The key difference between NPP 7.2 and the new Australian Privacy Principle (**APP**) 9.2 is that the latter allows use of government related identifiers by organisations in different circumstances, including where "*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 activities or functions*." A government related identifier is defined as follows:

government related identifier of an individual means an identifier of the individual that has been assigned by:

(a) an agency; or

(b) a State or Territory authority; or

(c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or

(d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

The current DVS access management policy limits commercial access and use to businesses operating under legislated client identification requirements. This restriction was informed by the prohibitions and permissions of the Privacy Act (NPPs 7.2, 2.1). In the light of the privacy reforms the Commonwealth Attorney-General's Department (**AGD**) is reviewing DVS access policies and is considering in particular potential privacy risks in expanding the range of businesses eligible for DVS access as may be permitted under the APPs.

This Privacy Impact Assessment report addresses the privacy benefits and risks associated with a greater number of private sector users having access to the DVS. It makes a number of recommendations to address privacy risks. There are also recommendations in relation to compliance issues.

For ease of reference, a glossary is provided in Schedule 1.

2. Executive summary

In short, we consider that expanded private sector access is legally permissible and that privacy risks can be appropriately managed and mitigated in accordance with the recommendations in this report.

2.1 The legislative test for use or disclosure of a government related identifier

Verifying documents through the DVS has a number of significant privacy advantages. It is far less privacy-intrusive than many of the existing tools of identity verification and, accordingly, increased access to and use of the DVS is desirable from a privacy perspective. However, a private sector organisation cannot be given access to the DVS unless use of the DVS by the organisation would comply with APP 9, that is:

a) 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 activities or functions (APP 9.2(a)); 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 (APP 9.2(b)); or

c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order (APP 9.2(c)); or

d) a permitted general situation (as defined in s 16A of the Privacy Act) exists in relation to the use or disclosure of the identifier (APP 9.2(d)); or

e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 9.2(e)); or

f) regulations about adoption, use or disclosure apply (APP 9.2(f)).

In order for a private sector organisation's use of the DVS to satisfy APP 9.2(a) (being that 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 activities or functions), we consider that:

- the prospective user's activities or functions in question must be legitimate for that type of entity (assessed from the perspective of a reasonable person); and
- identification of an individual or being presented with the details of an evidence of identity document must be reasonably necessary for the prospective user's activities or functions (assessed from the perspective of a reasonable person); and
- verification of the evidence of identity document - that is, use of the DVS - must itself be reasonably necessary (assessed from the perspective of a reasonable person).

2.2 A policy that will ensure that users are not given access unless there is clear compliance with APP 9

We recommend that there be clear, defensible criteria for assessing whether a prospective user falls within APP 9.2, in particular APP 9.2(a), that is whether using and/or disclosing government related identifiers is reasonably necessary for the organisation to verify the identity of individuals for the purposes of the prospective user's activities or functions. It is not enough that it be convenient or desirable, it must objectively be reasonably necessary. "Reasonably necessary" does not mean "absolutely necessary".

In our view, use of the DVS by a private sector organisation would fall within APP 9.2 if:

a) the organisation cannot lawfully perform its legitimate functions or activities without verifying individuals' identity. A prospective user is likely to fall within APP 9.2 if there is a Commonwealth, State, Territory or local government requirement that the prospective user know who their customer is.

b) the organisation has specific obligations to an agency or a State or Territory authority to verify identity.

c) the prospective user has a responsibility to protect the public or some section of the public, and identification is reasonably necessary for that activity or function.

d) it would not be reasonable to expect an organisation to perform its legitimate functions or activities without verifying individuals' identity.

There may be other circumstances in which an organisation would be able to use the DVS without contravening APP 9 but we recommend that the policy restrict access to situations in which an exception to APP 9 is clearly made out as the DVS should not facilitate a breach of the Privacy Act. We note that participating in the DVS in the absence of an access policy that would reasonably protect against a breach of APP 9 may constitute a contravention of APP 11 by an agency. We also note that there is no legal obligation to provide access to the DVS to any organisation.

3. Privacy risks identified and recommendations to mitigate those risks

3.1 Risk of unauthorised access or disclosure (that is, use of the DVS that would not comply with APP 9)

Issuing agencies may contravene the Privacy Act if the DVS does not contain reasonable measures to protect information held by agencies from unauthorised access or disclosure (APP 11). This could arise if a user breaches APP 9 in using the DVS.

The existing access policy meets the obligation in APP 11 as users who have legislated customer identification requirements are likely to fall within APP 9.2(b) and/or (c). As APP 9.2 permits use or disclosure of government related identifiers in a wider range of circumstances than legislated customer identification requirements, it is legally permissible to expand private sector access. However, this gives rise to a new risk of unauthorised access or disclosure. Participating agencies must ensure that the new access policy protects against unauthorised access or disclosure.

Our recommendations to mitigate the risk of unauthorised access or disclosure are as follows:

Recommendation 1

All prospective users must "opt in" to the Privacy Act to ensure that all users are required to comply with the Privacy Act.

Clause 11 of the DVS Business User Terms and Conditions of Use provides that "*You must ensure that your use of the DVS and Information Match Data complies with the Privacy Act 1988*". AGD has had a practice of ensuring that prospective DVS users have a privacy policy in place. However, with the expected increase in the number of private sector DVS users, AGD may not have capacity to continue this practice for all future applications. If Recommendation 1 is not adopted, there is a risk that a user who is not covered by the Privacy Act may argue that their use complies with the Privacy Act (not being required to meet certain conditions). The Gateway Service Provider Terms and Conditions of Use do not contain this provision. We recommend that the DVS Business User Terms and Conditions of Use and

Gateway Service Provider Terms and Conditions of Use both be amended to include a condition to the effect that:

> ***"You agree to be bound by and comply with the Privacy Act 1988 (Cth) including the Australian Privacy Principles, in respect of your access to and use of the DVS and Information Match Data, whether or not the Privacy Act 1988 (Cth) would otherwise apply to you".***

We also recommend that users and GSPs be required to register their choice to be treated as organisations with the OAIC in accordance with s 6EA of the Privacy Act.

Recommendation 2

Each of the document issuing agencies, including the State and Territory agencies, should consider the privacy implications with respect to their participation in the DVS.

This recommendation is to ensure that participating agencies consider whether the measures that will be in place are sufficient to protect the information they hold in the context of their own legislation.

Recommendation 3

A review of the DVS be conducted 2 years after any expansion of access to the private sector that has regard to any complaints received, any security breaches identified or reported, and any known breaches of the Privacy Act.

This recommendation will allow participating agencies to ascertain whether there has been any unauthorised access or disclosure or misuse, interference and loss arising from the expansion of private sector access in practice and to identify any further reasonable measures that should be put in place to protect the information they hold.

Recommendation 4

No private sector organisation should be given access to the DVS unless its use of the DVS would comply with APP 9. In relation to APP 9.2(a), a private sector organisation will have a reasonable need to use the DVS in order to verify the identity of individuals for the purposes of its activities or functions if:

- **the prospective user's activities or functions in question are legitimate for that type of entity (assessed from the perspective of a reasonable person); and**
- **identification of an individual or being presented with the details of an evidence of identity document is reasonably necessary for the prospective user's activities or functions (assessed from the perspective of a reasonable person); and**
- **verification of the evidence of identity document - that is, use of the DVS - is reasonably necessary (assessed from the perspective of a reasonable person).**

Recommendation 5

Any revised access policy should contain clear, defensible criteria for giving a prospective user access to the DVS which should accord with the language of the statute. This would include:

- **the organisation cannot lawfully perform its legitimate functions or activities without verifying individuals' identity.**
- **the organisation has specific obligations to an agency or a State or Territory authority to verify identity.**
- **the prospective user has a responsibility to protect the public or some section of the public, and identification is reasonably necessary for that activity or function.**
- **it would not be reasonable to expect an organisation to perform its legitimate functions or activities without verifying individuals' identity.**

We note that the policy could specify classes of organisations that would meet the policy requirements, or provide that organisations with particular characteristics or functions would ordinarily meet the policy.

3.2 Risk of misuse, interference and loss of personal information

Issuing agencies may contravene the Privacy Act if the DVS does not contain reasonable measures to protect information held by agencies from misuse, interference and loss (APP 11). This could arise if a user misuses or loses the personal information obtained through the DVS check.

This is an existing risk that would be increased if private sector access is increased. If private sector access is significantly increased, the risk of misuse, interference and loss is commensurately increased.

We note that the types of misuse, interference and loss of personal information obtained through a DVS search are speculative. The only examples we have been provided are guessing details (rather than verifying details provided by an individual) and using the information for a secondary purpose. Nonetheless, in keeping with the DVS's long-standing commitment to privacy, we consider that proper privacy safeguards be in place before any such risks materialise.

Clauses 8.1, 8.3, 8.5, 10, 11, 13, 16, 18, 24 and 25.2 of the DVS Business User Terms and Conditions of Use and clauses 2, 11.5, 11.6, 13, 14.3, 14.4, 17, 18, 19 of the Gateway Service Provider Terms and Conditions of Use all protect against misuse, interference and loss. Clause 7 of the DVS Business User Terms and Conditions of Use and clause 10 of the Gateway Service Provider Terms and Conditions of Use require that users and Gateway Services Providers (**GSPs**) (respectively) strictly comply with all instructions and guidance provided by the AGD. AGD's instructions include the extensive security requirements contained in the DVS Supporting Materials: Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013; see also *Document Verification Service: An Overview* (V4 December 2013). These security requirements include technology control minimum standards, employment screening, requirements to log activity and transactional data to enable monitoring for and reporting of security breaches, requirements to report security incidents or information security events to the DVS Operations Manager and the DVS Manager, and a requirement to have a designated Security Incident Investigator responsible for notifying the DVS Hub Security Incident Investigator and DVS Manager of any DVS security incidents. The DVS Hub Security Investigator will then report on the incident to the DVS Manager who will subsequently advise the National DVS Advisory Board. Security

incidents may also be reported to appropriate external parties (such as the police or the OAIC).

While the extensive existing contractual and security arrangements meet agencies' APP 11 obligations in the context of the current access arrangements, we recommend that the safeguards in place be increased to meet the increased risk of increased access. The **principal means by which this could be achieved is by auditing of users' compliance**, on at least a spot-check or random basis.

Users and GSPs are already required to fully cooperate with any audit or verification process to check their compliance: clause 10 of the DVS Business User Terms and Conditions of Use and clause 13 of the Gateway Service Provider Terms and Conditions of Use.

Users and GSPs are required to submit annual (or more frequent) compliance statements which must, at a minimum, confirm that the user's (or GSP's) use of the DVS is in accordance with the Terms and Conditions of Use and the DVS Supporting Material or, if the user did not fully comply with the Terms and Conditions of Use and DVS Supporting Material, what actions have been or are being taken to address the contravention: Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at sections 4.7 and 4.8.

GSPs are audited annually by independent auditors for compliance with the DVS terms and conditions (most users accessing the DVS through a GSP). However, currently users are audited on the basis of risks identified in assessing their compliance statements. We recommend auditing users. We appreciate that it would be impractical to regularly audit every user but we recommend putting in place a process by which any users who have been identified as a security or privacy risk are audited and all users may be randomly selected for a compliance audit or "spot-check". This may have implications for compliance costs but could be built into pricing structures and passed on to users.

The existing information and access security measures are in accordance with industry best practice and we have assumed that this will continue to be the case. Accordingly, we have not made recommendations about information security.

The existing security measures protect against information security breaches (subject to our recommendation of increased auditing). However, there is currently no formal complaints process by which an individual could complain about misuse of their personal information or a breach of privacy.

Our recommendations to mitigate the risk of misuse, interference and loss are as follows:

Recommendations 1 and 3 above mitigate against this risk.

Recommendation 6

There should be auditing of users' data security and privacy compliance in relation to their use of the DVS on at least a spot-check basis. Suspension or termination should be considered if a user has failed to report a data security or privacy breach to the DVS Hub Security Incident Investigator or the DVS Manager of which the organisation should reasonably have been aware, or if a user has reported a data security or privacy breach but has not put in place reasonable measures to ensure it is not repeated.

Recommendation 7

There should be a formal complaints process managed by AGD whereby individuals can complain to AGD about the actions of user organisations or GSPs in relation to their use of the DVS or use of information obtained though their use of the DVS. Users should be required to tell individuals where to find details of the complaints process. We recommend that the complaints process be detailed on the DVS website and also provide information as to other complaints mechanisms, such as the OAIC and State and Territory privacy regulators.

Recommendation 8

The operations of the DVS should be regularly reviewed and include consideration of any complaints received and reviews undertaken.

3.3 Risk that the individual has not provided free and informed consent to the DVS check

Issuing agencies may contravene the Privacy Act in responding to a DVS check without the informed consent of the individual (APP 6). Informed consent is also important for compliance with APPs 3 and 5. APPs 3.6 and 6.1 will be satisfied by issuing agencies so long as the consent is informed.

This is an existing risk that would be increased if private sector access is increased. We do not consider that the existing mitigations are adequate to meet the increased risk.

Clauses 12.2 and 12.3 of the DVS Business User Terms and Conditions of Use and clause 14.1 of the Gateway Service Provider Terms and Conditions of Use mitigate against this risk by requiring that DVS checks must be undertaken with the informed consent of the person whose information is being used. However, there is a risk that users might interpret clause 8.6 of the DVS Business User Terms and Conditions of Use as preventing them telling individuals about the existence and use of the DVS. The Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 provided to users and GSPs suggests the following wording at section 10.1: "*Information provided as evidence of your identity in/with this application will be checked with the document issuing agencies*" which does not explain the existence of or the role of the DVS.

In order to ensure that agencies comply with APP 6.1 and do not facilitate a contravention of APPs 3 or 5, we recommend requiring private sector users to provide individuals who present their document details for verification with an approved, concise plain English explanation of what the DVS does, how their details will be used, and what information will be contained in the DVS request and response. Users should be required to tell individuals where they can find further information about the DVS, such as a page on the DVS website, so that consumers understand the nature of the DVS as well the benefits it provides. The statement should be short so that it can be read out over the telephone.

In addition to a uniform DVS notification and consent that private sector users must provide to the individual, we recommend that each user be contractually required to provide the individual with information in the specific context of the prospective user organisation's activities or functions that addresses any alternatives to having their document details verified, the consequences if the individual does not consent to the DVS check (such as being unable to access the particular goods or services sought), and the consequences if the DVS returns a non-match response.

We recommend that there should be publicly available information on what individuals can do to access, and correct, information about them, such as the contact details of the issuing agencies. If the individual provides the document details online, there should be a link to the page containing the relevant information, such as the contact details of the issuing agencies. If the individual provides the document details online, there should be a link to the page containing the relevant information. The information should be centralised on the DVS website so that individuals can easily ascertain which government agency holds the information.

Our recommendations to mitigate the risk that an individual has not consented to the DVS check are as follows:

Recommendation 7 above mitigates against this risk.

Recommendation 9

In order to ensure informed consent, users should be contractually required to provide individuals who present their document details for verification with an approved, concise plain English explanation of what the DVS does, how their details will be used, and what information will be contained in the DVS request by the user and response by the agency. Users should be required to tell individuals where they can find further information about the DVS, such as a page on the DVS website, so that consumers understand the nature of the DVS as well the benefits it provides.

At a minimum, we consider that users should be contractually required to tell individuals words to the effect of:

"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 webpage such as www.dvs.gov.au] or by telephoning/writing to [insert telephone number, fax number or post office box number]".

Recommendation 10

Each user should be contractually required to provide the individual with a short, plain English explanation in the specific context of the prospective user organisation's activities or functions that addresses any alternatives to having their document details verified, the consequences if the individual does not consent to the DVS check (such as being unable to access the particular goods or services sought), and the consequences if the DVS returns a non-match response.

An example of this would be "*If you do not provide your driver's licence or passport number or your document is not verified by the Document Verification System, we may not be satisfied as to your identity and you may not be able to open an account with us online*".

The current Document Verification Service Business User Terms and Conditions of Use (**Attachment 2**) require that users obtain express and informed consent (clause 12). This recommendation could be implemented by amending clause 12.2 as follows:

"1.2 is informed of:

(a) the purpose for which that information is sought and will be used by you (including that the information will be subject to an Information Match Request in relation to relevant Official Record Holder information, and that a corresponding Information Match Result will be provided via the use of third party systems);

(b) any alternatives to the Information Match Request;

(c) any consequences if the individual does not consent to the Information Match Request; and

(d) any consequences if the details in a Supported Document cannot be matched with the relevant Official Record Holder information."

Recommendation 11

There should be publicly available information on what individuals can do to access, and correct, information about them, including the contact details of the issuing agencies.

This recommendation could be implemented by ensuring that the DVS website contains the contact details of the issuing agencies.

We note that the above recommendations address privacy risks. However, we note that it was submitted to us that consumers are likely to be uncomfortable with widespread use of the DVS or use of the DVS where the need to verify identity documents is not obvious. We consider that public confidence in the DVS (in the context of greater public sector access) is likely to be increased by ensuring that there is a robust access policy and that there are stringent privacy protections. In that context, we note that privacy has been a significant consideration in the design and operation of the DVS since its inception.

4. About this PIA

4.1 What is a privacy impact assessment?

A Privacy Impact Assessment, or **PIA**, is an examination of a project from a privacy perspective. The primary purposes of a PIA are to:

a) examine how personal information is collected, used and disclosed as part of a project;

b) analyse the impacts of the project on personal privacy; and

c) identify and recommend options for managing, reducing or removing those impacts.

PIAs are conducted to ensure that privacy issues are fully considered in the design and implementation phase of a project. PIAs help ensure that projects meet privacy requirements in legislation and are also consistent with broader community privacy expectations.

4.2 The approach of this PIA

This PIA has been prepared broadly in accordance with the *Privacy Impact Assessment Guide* (Office of the Australian Information Commissioner, May 2010) (the **PIA Guide**). That guide recommends that PIAs be conducted in five key stages, as shown diagrammatically below.

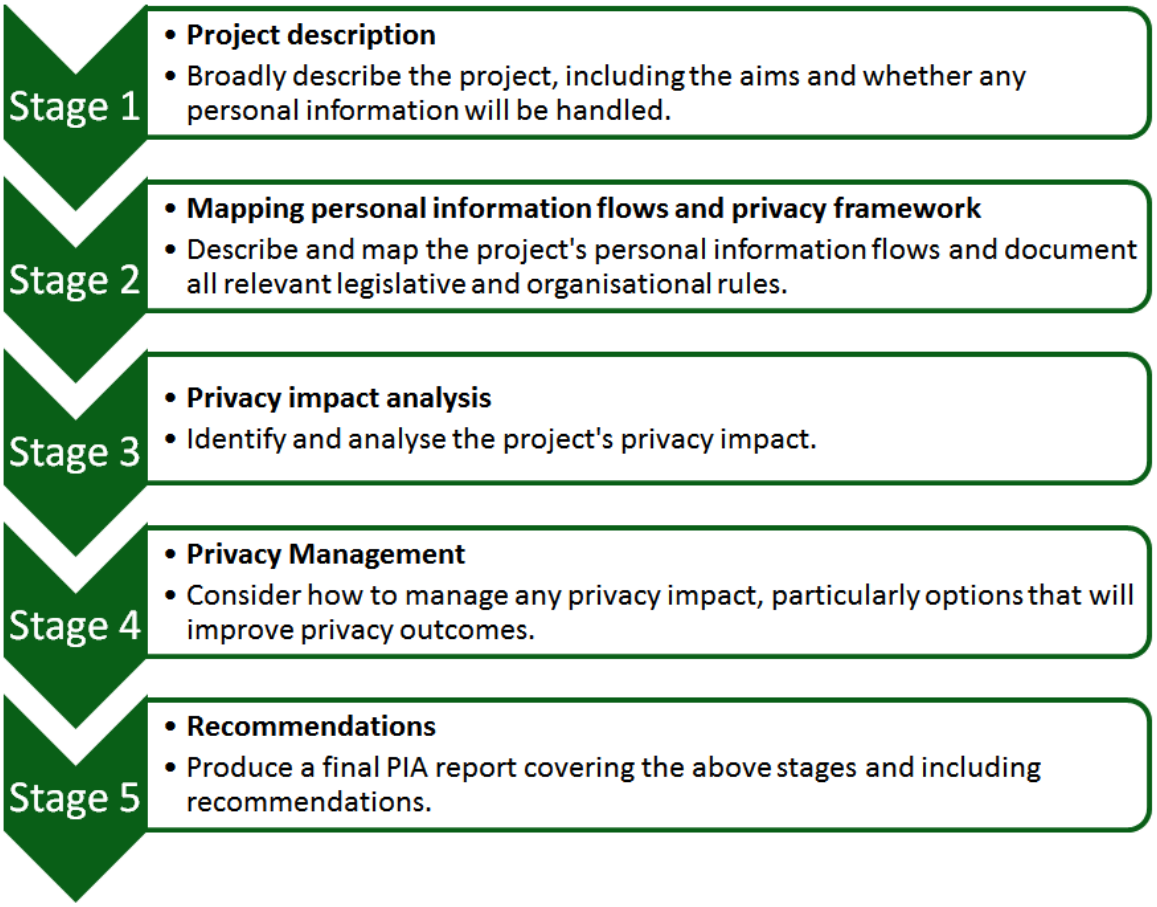


Figure 2—PIA stages (Source: PIA Guide, p xii)

The PIA in this report is set out thematically; the PIA explores particular areas, themes and risks of expanded commercial sector access. To aid readability, the privacy impact analysis and privacy management options are dealt with together in each of the themes explored in this PIA.

4.3 Relevant Documents

We had the benefit of reading the documents set out in Schedule 2.

We also had the benefit of reading written submissions prepared following the consultation process described at 3.4 below.

4.4 Consultation

In the course of this PIA, we consulted with the AGD, the OAIC, government document issuing agencies, users of the DVS (including government agencies and prospective private sector organisation users), and privacy experts and advocacy groups. We did this by emailing the written invitation to comment at **Attachment 1** on 22 January 2014. We invited those consulted to provide a written preliminary indication of their views by 7 February 2014 and to meet with us in the week commencing 10 February 2014. Most of the agencies and organisations consulted took the opportunity to meet with us. We requested final comments or submissions by 28 February 2014.

We invited a number of Commonwealth and State and Territory agencies to comment, including users, document issuing agencies and agencies who were both users and document issuing agencies, including the Department of Foreign Affairs and Trade, the Department of Human Services, the Department of Immigration and Border Protection, the Australian Taxation Office, the New South Wales Attorney General & Justice - Registry of Births, Deaths & Marriages, and the Victorian State Revenue Office.

We invited a number of users of the DVS, including private sector organisations and Gateway Service Providers to comment, including Veda, Edentiti, the Commonwealth Bank, and Telstra.

We invited a number of independent advocacy groups and privacy experts to comment, including the Australian Privacy Foundation, Electronic Frontiers Australia, Liberty Victoria, and Nigel Waters.

At the suggestion of the OAIC and two of the privacy experts consulted, we forwarded the invitation to comment to a number of consumer advocacy groups on 12 February 2014, including the Consumers' Federation of Australia, the Consumer Credit Legal Centre, Choice, and the Australian Communications Consumer Action Network.

Unfortunately, in some cases owing to timing, resourcing constraints or other issues, we did not receive any specific feedback from the consumer groups consulted, only general principles relating to consumer protection. However, we did have regard to the OAIC *Community Attitudes to Privacy Survey Research Report* 2013.

We asked the following questions:

Questions for consultation

Generally:

- Without the DVS, what other methods (paper-based, electronic, etc.) can organisations use to verify the identity of individuals?
- What might be the downstream privacy impacts of those other identification processes (document copying, record keeping, etc.)?

In relation to each proposal:

- What impact do the amendments to the Privacy Act 1988 (Cth) have on the lawfulness of the proposal?
- In what circumstances could the proposal have a positive impact for individuals whose identities are being verified by an organisation?
- In what circumstances could the proposal have a negative impact for individuals whose identities are being verified by an organisation?
- In what ways can any negative impacts could be managed?
- What security or access controls should be adopted if the proposal is adopted?
- What information should individuals be given about the results from the DVS if the proposal is adopted?

Please also address any other issues you see with the proposal.

We acknowledge with gratitude the written submissions we received from agencies, users and privacy advocates. In particular, we had the assistance of the written submission of the OAIC, and we had the assistance and expertise of the AGD.

4.5 Applicable legislation

This PIA analyses access to the DVS against the provisions of the Privacy Act. In this regard, this PIA focuses on the APPs which commenced on 12 March 2014. In addition to the Privacy Act, other legislation will also affect the operation of the DVS. However, this PIA focuses only on obligations which arise under the Privacy Act.

4.6 State and Territory legislation

We are instructed that a separate PIA will be conducted in respect of applicable State and Territory legislation. The State and Territory agencies that allow the DVS to verify the details of documents and the applicable State and Territory legislation is set out at Schedule 3.

4.7 Scope, limitations and assumptions

This PIA has been set out on the basis that the DVS continues to be managed by the AGD on behalf of all jurisdictions as part of the Council of Australian Governments' National Identity Security Strategy. The DVS Hub is currently hosted by a Commonwealth agency (Centrelink) but this PIA recognises that the DVS Hub might one day be hosted by a private sector provider on behalf of AGD.

The focus of the PIA from a privacy compliance perspective is on those transactions within the DVS rather than what users may do with the information. However, from a privacy impact and management point of view, information flows are analysed from a broader perspective including reasonable expectations of privacy.

The information flows and system design of the DVS as described in this PIA is based primarily on the documents described in Schedule 2.

5. Description of the DVS

5.1 Evidence of Identity Documents

There are a range of documents verified by the DVS which commonly serve as "identity documents" in the community. We note that it was submitted to us by a number of individuals or organisations consulted that it is convenient but incorrect to describe these documents as identity documents. As the documents verified contain information that commonly functions for identifying purposes, such as driver's licences, and passports, in this document we will refer to **evidence of identity documents**.

The DVS does not verify that a document presented is authentic. Rather, it confirms that the details contained (or said to be contained) in the document match (or do not match) the details held by the agency that issued the document.

5.2 Background

In 2005, the Council of Australian Governments (**COAG**) endorsed the development of a National Identity Security Strategy (**NISS**) to protect the Australian community from identity theft. In doing so COAG also agreed to establish a Document Verification Service (DVS) to combat the misuse of false and stolen identities.

One of the primary aims of the NISS in establishing the DVS was to ensure that government agencies could confirm that the details of an evidence of identity document issued by another agency were correct. The DVS does not confirm whether a document is genuine or not but it does confirm that the information contained in the document matches the information held by the document issuing agency.

The DVS has been available to some government agencies (principally Commonwealth agencies) since 2008.

Since December 2013, the DVS has been available to those private sector organisations that are required under Commonwealth law to know the identity of their customers, primarily organisations involved in banking, credit reference, finance, superannuation, telecommunications, and gambling. Legislation that requires organisations to identify their customers includes:

a) Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (Cth);

b) Financial Transactions Reports Act 1988 (Cth) and Financial Transactions Reports Regulations 1990 (Cth);

c) Superannuation Industry (Supervision) Act 1993 (Cth) and Superannuation Industry (Supervision) Regulations 1994 (Cth);

d) Retirement Savings Account Act 1997 (Cth) and Retirement Savings Account Regulations 1997 (Cth);

e) The former Credit Reporting Code of Conduct under the Privacy Act and now the Credit Reporting Privacy Code (**CR Code**);

f) Aviation Transport Security Act 2004 (Cth) and Aviation Transport Security Regulations 2005 (Cth);

g) Maritime Transport and Offshore Facilities Security Act 2003 (Cth) and Maritime Transport and Offshore Facilities Security Regulations 2003 (Cth); and

h) Telecommunications Act 1997 (Cth) and Telecommunications (Service Provider - Identity Checks for Prepaid Mobile Carriage Services) Determination 2013 (Cth).

All DVS users including private sector organisations must be approved by the DVS Advisory Board. The DVS Advisory Board currently undertakes a due diligence process before approving private sector users, to confirm that the prospective user is covered by the Privacy Act, has customer identification obligations under law, and has its registration or licensing overseen by local regulatory authorities such as the Australian Transaction Reports and Analysis Centre (AUSTRAC), Australian Prudential Regulation Authority (APRA), Australian Securities and Investments Commission (ASIC) or the Australian Communications and Media Authority (ACMA).

Since December 2013, the DVS has also been available to approved GSPs. GSPs act as agents for users, either allowing approved users to search the DVS through the GSP's interface (DVS application) or conducting both the customer identification and the technical transactions on behalf of users. GSPs allow users to avoid the expense of developing their own DVS interface and complying with security protocols. GSPs also facilitate cheaper search fees under a volume discount - the general access rate being $1.40 per search with volume-based discounting reducing that cost to between $0.65 - $1.20.

Government agencies and GSPs have their own interfaces with the DVS. Private sector organisations may have direct access to the DVS through their own interface or may use the services of a GSP.

The governance arrangements are summarised in the *Document Verification Service: An Overview* (V4 December 2013). The contractual terms of access are contained in the Document Verification Service Business User Terms and Conditions of Use (**Attachment 2**) and Document Verification Service Gateway Service Provider Terms and Conditions of Use (**Attachment 3**) and are summarised in Schedule 4. We understand that the instructions and guidance provided by the AGD (that GSPs must comply with pursuant to clause 10 of the Gateway Service Provider Terms and Conditions of Use, and users must comply with pursuant to clause 7 of the Business User Terms and Conditions of Use) currently include the DVS Supporting Materials.

Potentially, one consequence of the new APPs which took effect 12 March 2014 pursuant to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) may be to increase the number of private sector organisations that seek to verify evidence of identity documents via the DVS as the reforms affect the previous restrictions on the use of government related identifiers pursuant to the repealed NPPs, particularly NPP 7.2. The AGD is considering the

privacy implications of a greater number of private sector organisations requesting access to the DVS.

5.3 What is the DVS?

The DVS is a secure online system that enables organisations to verify the information contained in evidence of identity documents with the records of the document issuing agencies (such as Commonwealth agencies and State and Territory Registries). The evidence of identity documents that can be verified against the records of the issuing agencies include:

a) birth certificates;

b) certificates of registration by descent;

c) change of name certificates;

d) citizenship certificates;

e) driver licenses;

f) marriage certificates;

g) Medicare cards;

h) passports;

i) Immi Cards; and

j) visas.

The DVS is not a database and does not itself store any personal information for any longer than is required to complete the search.

The DVS is available 24 hours per day, 7 days per week and generally provides a response within a few seconds.

5.4 What is the information flow?

There are five participants in a DVS transaction:

a) **The individual—**The individual wishes to access or obtain a benefit, product or service from a user organisation. To do so, he or she must provide evidence of their identity in the form of the physical document, a copy of the document or the details of an evidence of identity document. This is done online, by telephone, in writing or in person.

b) **The user—**The user enters the details of the evidence of identity document (either directly or through a GSP - see below) into a DVS system or interface. The details are entered manually and then the request is sent securely by the user's interface to the DVS Hub.

c) **The gateway service provider (optional)—**The GSP allows users to interrogate the DVS through the GSP's interface (or DVS system). The GSP acts as the agent of the user.

d) **The DVS Hub**—The DVS Hub accepts the request from the user (or their GSP) using the Verification/Match Request Number (**VRN**) assigned by the user (or their GSP). The DVS Hub reformats and reroutes the request to the appropriate issuing agency with a new VRN. The DVS Hub receives a Y, N, S or D response back from the

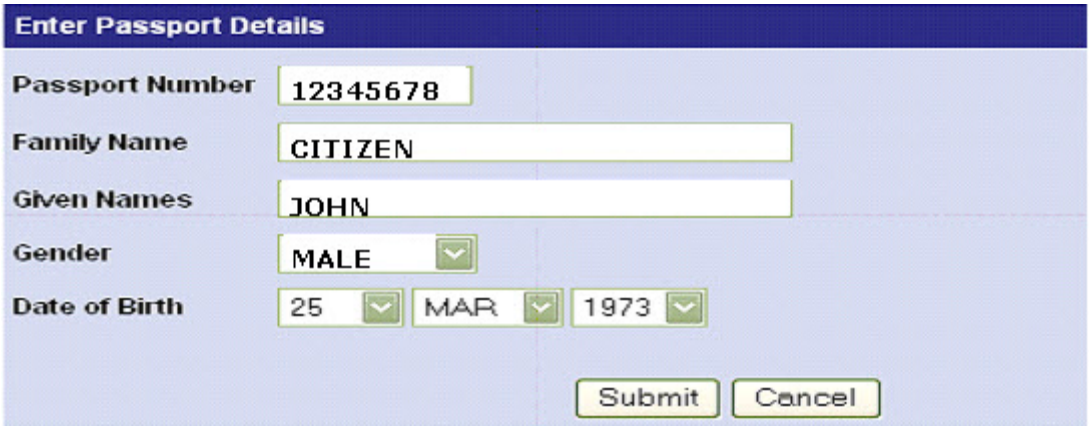
issuing agency with the second VRN. The DVS Hub then reformats and reroutes the response back to the user with the original VRN.

e) **The government document issuing agency**—The issuing agency receives the request from the DVS Hub, conducts an automated check of the details in the request against its own records, and sends a response to the DVS Hub being Y, N, S or D.

A search of the DVS involves the following steps:

- An individual provides the details of an identity document to establish his or her identity, either by presenting the physical document or a copy of the document, by providing the details by telephone or online, or by setting out the details in a written application. The individual consents to a DVS user checking the details of the identity document.
- The DVS user then enters the details of the identity document (for example, the passport number, family name, first name, gender and date of birth) into the DVS/The DVS user provides the details to the DVS via a GSP.

The following example is provided on the DVS website:



- The request is then sent to the DVS Hub, which is a technical router that allows DVS requests to be securely sent between users and issuing agencies, through a secure communications route.
- The DVS Hub encrypts the request and forwards it via a different secure communications route to the document issuing agency. A transaction number is assigned to it.
- The document issuing agency undertakes an automated check of the agency's data to ascertain whether the information provided matches the information held by the agency.
- The document issuing agency sends a response back to the DVS Hub via the same secure communications route as the request from the DVS.
- The DVS Hub re-encrypts the response and sends back to the user (or GSP) via the original secure communications route.
- The user will receive one of the following responses in respect of the entire request:
  - [**Y**] – all of the details entered match the details of the issuing agency's records and the document is still valid (that is, not expired or cancelled).

- [**N**] – one or more of the details do not match the details of the issuing agency's records or the details match but the document is no longer valid (that is, it has expired or it has been cancelled).

- [**S**] - system availability error. The DVS request cannot be sent to the issuing agency within 60 seconds or a system availability problem prevents the response being returned. A user should resubmit the request at a later time.

- [**D**] - data range error. This indicates that the request includes data that has not been electronically captured by the issuing agency. For example, older documents may not have been electronically captured in particular jurisdictions.

6. What is proposed in terms of expanded private sector access?

The DVS is already available to private sector organisations with a legislated requirement under Commonwealth legislation to identify their customers. The AGD anticipates that the reforms to the Privacy Act will lead to a greater number of private sector organisations requesting access.

Expanded use of the DVS offers significant privacy benefits over more intrusive identity verification methods, avoiding the need for organisations to keep copies of evidence of identity documents. Expanded DVS use is also likely to facilitate online transactions without the need for hardcopy evidence of identity documents to be provided.

However, the AGD and the issuing agencies must not facilitate or assist in a contravention by a user of APP 9 and accordingly must put in place arrangements to limit use by organisations to circumstances where the use of the DVS would comply with APP 9. Further, allowing private sector access without taking reasonable steps to prevent a breach of APP 9 might constitute a breach of APP 11 by participating agencies.

In our view the existing access policy (restricting access to organisations with a legislative requirement) complies with the APPs and would not give rise to a risk that an agency would breach APP 11. APP 9 clearly permits a broader range of circumstances than a legislative requirement (which is specifically included in APP 9.2(c)). Expanding private sector access beyond the existing access policy is therefore legally permissible. However, the DVS must take reasonable steps (such as a clear access policy) to ensure that users are not granted access unless they would comply with APP 9.

The key difference between APP 9.2 and the previous NPP 7.2 is found in APP 9.2(a) which allows use of government identifiers by organisations in different circumstances, including where "*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 activities or functions*."

The AGD has commissioned this PIA in order to understand circumstances in which, under the APPs, use or disclosure of a government related identifier in a DVS check can occur, and to explore potential privacy risks in expanding the range of private sector organisations eligible for DVS access as may be permitted under the APPs.

6.1 What types of organisations may request access to the DVS?

Potentially, any private sector organisation might see a benefit in verifying evidence of identity documents through the DVS.

In the course of consultation, a number of examples were suggested to us which include:

- utilities providers, to whom customers must provide "acceptable identification" under National Energy Retail Rules;

- the real estate sector, in the context of assessing the suitability of tenants, and especially in the context of the Australian Registrars' National E-Conveyancing Council (**ARNECC**) and the implementation of the regulatory framework for National E-Conveyancing (the Electronic Conveyancing National Law);
- sensitive employment environments;
- universities and other education providers (in the context of avoiding plagiarism and cheating);
- registration of health professionals;
- second hand goods dealers;
- car rentals and car share arrangements;
- hotels with safety deposit boxes and gaming machines;
- child protection;
- personnel screening agencies;
- online dating; and
- online gambling.

7. Benefits in the DVS

7.1 Privacy

The DVS has promoted privacy protection since its inception, incorporating privacy protection into its design and operation, and undertaking regular PIAs. The issuing agencies also take privacy obligations very seriously.

The DVS is far less intrusive from a privacy perspective that existing methods of identity verification, such as screen-scraping (getting an individual to enter their details into a public-facing third party database), web-harvesting, transaction history analysis or keeping photocopies or scanned copies of evidence of identity documents.

The DVS is safer and has more stringent security requirements than paper-based verification where photocopies might be stored in a filing cabinet or even a shoe box.

A record held by a user that indicates that (for example) James Brown's details were successfully matched contains far less personal information than a copy of James Brown's passport which would indicate his name, age, perhaps ethnicity, his driver licence which would also indicate his address and perhaps that he requires glasses, or his Medicare card which would indicate his family unit (such as a partner, children, and even whether he lives in a blended family or step family).

The DVS reduces the risk of identity theft by allowing the veracity of documents to be checked against the issuing agency's records (and potentially by reducing the value of false documents).

The DVS can facilitate greater privacy in customer identification procedures for the purposes of online transactions or applications for benefits and services.

This PIA is concerned with privacy benefits. However, we note that there are other advantages to the DVS which are also important to individuals.

7.2 Identity security

We understand that identity crime is amongst the most prevalent crime types in Australia. Recent research by the Australian Institute of Criminology indicates that:

- almost 1 in 10 people experienced misuse of their personal information in the previous 12 months,
- 1 in 5 people experienced misuse of their personal information at some point in their lives; and
- 5% of people experienced identity crime or misuse resulting in a financial loss in the previous 12 months.[1]

AGD estimates that identity crime directly affects around 1 million Australians each year and has an annual economic impact on individuals, businesses and governments of at least $1.6 billion.

In its 2012 Organised Crime Threat Assessment, the Australian Crime Commission rated identity crime as a key enabler of serious and organised crime, which in turn costs Australia around $15 billion annually.[2]

A significant proportion of identity crime is facilitated by use of stolen, counterfeit or fraudulently obtained identity documents (e.g. documents obtained by using false or stolen information). Available information on the nature and extent of data breaches, together with the cost of fraudulent identity documents, indicates that these documents and/or the information needed to fraudulent manufacture or acquire then are readily available to criminals.

For example, a fraudulent Medicare card can be obtained for as little as $80 and driver licences for around $350.[3] The 22 Australian incidents examined in the 2011 Ponemon Study involved the theft of an average of 19,000 records per incident, at an average cost of $138 per record. This compares to the 59 voluntary data breach reports in 2011-12 received by the OAIC that cost an average of $133 a record.[4]

The DVS plays an important role in preventing identity crime by ensuring that the veracity of information on identity documents can be confirmed directly and securely with the document issuing agency. Documents that have been reported stolen, have been cancelled or have expired cannot be successfully verified (returning an N response).

Greater use of the DVS is likely to reduce the utility of fraudulent or stolen identity documents in facilitating identity crime which in turn is likely to increase the reliability of government documents.

---

[1] Russel G Smith and Alice Hutchings, *Identity crime and misuse in Australia: Results of the 2013 online survey* (Australian Institute of Criminology, February 2014) pp 48-50.

[2] Australian Crime Commission, *Organised Crime in Australia Report* (2013) pp 6, 13.

[3] Commonwealth Attorney-General's Department, *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot* (2014) p 6.

[4] Commonwealth Attorney-General's Department, *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot* (2014) p 23.

7.3 Electronic commerce and efficiency

The DVS is likely to be of significant benefit in facilitating online transactions as (inter alia) banking, commerce, dealings with government, and applications are increasingly conducted online. A "Y" result in an online DVS check is likely to facilitate an individual's ability to transact online, such as opening a bank account or selling shares, and enable him or her to do so faster.

A recent study by the Secure Identity Alliance and Boston Consulting Group estimated that e-Government services, enabled by trusted digital identities, are set to yield an estimated $50 billion in annual global savings by 2020.[5]

The DVS is also an important tool in reducing the regulatory impacts on business, by minimising compliance costs that can flow from regulatory obligations for customer identification, such as those in anti-money laundering and some telecommunications regulations.

Use of the DVS in the telecommunications sector, to support sales of pre-paid mobiles SIM cards, has been estimated to achieve time and cost savings of up to 70 per cent, compared to other manual processes for verifying customer identities.[6]

8. How personal information is collected, used and disclosed in a DVS transaction

The types of personal information collected, and the ways in which that information is used and disclosed by the DVS, are set out below.

Collection	The user, or GSP on the user's behalf, will collect the personal information being the document details from the individual, in person, by telephone, in writing or online. The personal information is arguably collected by the DVS or by the issuing agency via the DVS from the user or the GSP, albeit for a matter of seconds (or less). Further personal information (being the response, as set out in relation to disclosure below) is arguably collected by the DVS from the issuing agency, again only for a matter of seconds (or less). Personal information (being the response) is collected by the user (or the GSP on the user's behalf) from the DVS or from the issuing agency via the DVS.
Use	Personal information collected by the user will be used to: • verify the details on the document (in this example, a passport) and, consequently: • verify the identity of the individual.

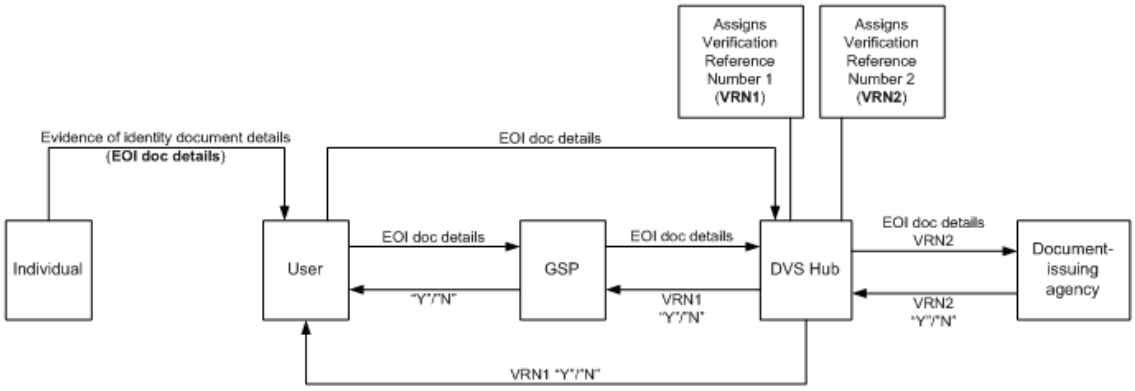
[5] Secure Identity Alliance and the Boston Consulting Group, *Enabling the eGovernment 2020 Vision: the Role of Trusted Digital Identity* (March 2014) p 3.

[6] Department of Broadband, Communications and the Digital Economy, *Regulation Impact Statement: Proposed Changes to Identity Verification Requirements for Prepaid Mobile Services* (February 2013) p 17.

Disclosure	The user (or a GSP on the user's behalf) will disclose the following personal information (the information will vary depending upon the document being verified but, to take the example of a passport): • the individual's passport number, for example 12345678; • the individual's surname, for example Brown; • the individual's given names, for example James; • the individual's gender, for example male; and • the individual's date of birth, for example 6 February 1978; and • the fact that the individual (James Brown) has presented the details of a passport to a user to be verified. A further inference might be drawn that James Brown is seeking a benefit or service of a kind provided by the user, for example a prepaid mobile phone. The agency discloses the following personal information via the DVS back to the user or GSP (at this stage - the possibility of field specific matching being the subject of a separate privacy impact assessment): • the individual holds a passport, the passport is still valid, his passport number is 12345678, his name is recorded on his passport as James Brown, he is recorded as male in his passport, and his date of birth is recorded in his passport as being 6 February 1978; or • one or more of those details is not correct (that is there is no passport with the number 12345678 and the first name James and the surname Brown and the gender male and the date of birth 16 February 1978) or the passport is no longer valid.

8.1 The flow of information between the user, GSP, DVS and issuing agency

The following diagram shows how information flows in the course of a DVS transaction.



8.2 Ensuring compliance with privacy obligations in relation to collection, use and disclosure

There is no specific legislative authority for the collection, use and disclosure of personal information as part of the DVS (and we are not aware of any plans to draft regulations for the purpose of APP 9.3). Therefore, the DVS will need to comply with the relevant APPs to ensure that the DVS complies with the AGD's and the issuing agencies' obligations under the Privacy Act.

Although the restriction on the use of government related identifiers in APP 9 applies to the users and the GSPs, the Commonwealth ought not facilitate a contravention of the Privacy Act by allowing use of the DVS in circumstances where use or disclosure by the organisation would not fall within an exception to APP 9.2. Further, there is a risk that agencies participating in the DVS might be found to have contravened APP 11 if reasonable steps (such as a robust access policy) are not taken to prevent a breach of APP 9.

A summary of the application of the relevant APPs to the DVS is set out below.

Relevant APP	**Rules contained in the relevant APP**	**Implications for the DVS**
Collection APP 3	Personal information must generally only be collected from the individual concerned. Personal information may be collected from someone other than the individual if it is unreasonable or impractical to collect from the individual (or, in the case of an agency, if the individual consents) (APP 3.6).	The user (or GSP on the user's behalf) collects personal information from the individual for the purposes of checking that information against the issuing agency's records using the DVS. The user (or GSP on the user's behalf) collects personal information from the issuing agency or the DVS, being the DVS response. The DVS arguably collects personal information from users and GSPs and from the issuing agency. The issuing agency arguably collects personal information from the DVS or from the user via the DVS. It is important that the individual consents to the information being disclosed to the DVS and by the DVS to the issuing agency, and consents to the response being disclosed by the issuing agency to the DVS and by the DVS to the user. After the initial point of collection from the individual presenting their details to be verified, collection from the individual would be unreasonable or impractical in the subsequent information flow.
	In the case of an agency, personal information may only be collected if it is reasonably necessary for, or directly related to, one or more of the agency's functions or activities (APP 3.1).	The DVS and the issuing agency will only be able to collect personal information to the extent that it is reasonably necessary for, or directly related to, their functions or activities. Verifying documents is directly related to identity security and the DVS is a key component of the NISS, one of the AGD's functions or activities. The issuing agency's functions and activities as issuer of the documents sought to be verified will support this collection.

Relevant APP	Rules contained in the relevant APP	Implications for the DVS
	In the case of an organisation, personal information may only be collected if it is reasonably necessary for, or directly related to, one or more of the organisation's functions or activities (APP 3.2).	We recommend ensuring that all DVS users are covered by the Privacy Act. To the extent that the collection by the user is from the DVS or the issuing agency, we consider that APP 3.2 will be met in circumstances where APP 9.2 is satisfied.
Notification of collection APP 5	At or before the time of collection, an APP entity must take steps to notify the individual of the matters set out in APP 5.2 or to otherwise make sure the individual is aware of those matters, including but not limited to the identity and contact details of the APP entity, the fact of the collection, and the purpose of the collection.	We consider that APP 5 will be met in circumstances where the individual is informed at the point of providing their evidence of identity document details that the information will be checked with the issuing agencies for the purpose of verifying the document details and that information on the participating agencies can be found on the DVS website (or other means of obtaining further information).
Use and disclosure APP 6	Information collected for a particular purpose cannot be used or disclosed for another purpose unless: • the individual consents; or • the individual would reasonably expect the information be used for the secondary purpose and, for information that is not sensitive information, the secondary purpose is related to the primary purpose.	The individual must expressly consent to the organisation disclosing information to the DVS and to the issuing agency, and expressly consent to the issuing agency disclosing information to the DVS and to the user. We recommend standard required wording.
Adoption, use or disclosure of government related identifiers APP 9	An organisation must not use or disclose a government related identifier (APP 9.2) unless: • 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 organisations activities or functions (APP 9.2(a)); • 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 (APP 9.2(b)); or • the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal	The Commonwealth (and other jurisdictions in the governance of the DVS) should not permit an organisation to use the DVS unless verification of the document would fall within APP 9.2.

Relevant APP	Rules contained in the relevant APP	Implications for the DVS
	order (APP 9.2(c)); or • a permitted general situation (as defined in s 16A of the Privacy Act) exists in relation to the use or disclosure of the identifier (APP 9.2(d)); or • the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 9.2(e)); or • regulations about adoption, use or disclosure apply (APP 9.2(f)).	
Security of Information APP 11	If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from: • misuse, interference and loss (APP 11.1(a)); and • unauthorised access, modification and disclosure(APP 11.1(b)).	All participating agencies must take reasonable steps to prevent misuse, interference and loss. We consider that the existing information security measures meet this obligation, although we recommend auditing of users on a spot-check basis. All participating agencies must take reasonable steps to prevent unauthorised access and disclosure. We consider that this will be met if all users are required to opt in to the Privacy Act and there is an access policy in place to ensure that only users whose use would comply with APP 9.2 are granted access. The current access policy protects issuing agencies from being found to have contravened APP 11. However, we consider that wider public sector access can be permitted so long as the access policy accords with APP 9.2.

The issues of consent and of "reasonably necessary" are discussed in further detail below.

8.3 Consent

In the absence of legislation which authorises the collection, use and disclosure of information, the operations of the DVS will need to comply with the relevant APPs. As set out in the table above, APP 3.6s and 6 are satisfied if there is consent.

As the Administrative Decisions Tribunal in NSW has noted (in relation to the operation of NSW privacy legislation), in order for consent to be valid, it must be '*freely given and informed*'.[7]

A great deal of the feedback we received related to the issue of consent and the need to ensure that individuals are informed of the existence of the DVS, the process involved in a DVS check, what happens if there is a negative response and any alternatives to having their details checked by the DVS. It was suggested to us that where a person has no choice but to provide information, it may be difficult to describe consent as '*freely given and informed*'.

We consider that APPs 3.6 and 6 will be satisfied by issuing agencies so long as the consent is informed.

8.4 APP 9

APP 9 restricts the use or disclosure of government related identifiers. A government related identifier is defined by s 6 to mean "*an identifier of the individual that has been assigned by: (a) an agency; or (b) a State or Territory authority; or (c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or (d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract*." A government related identifier would include a passport number, driver licence number, or Medicare number.

APP 9 provides:

> *Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers*
>
> *Adoption of government related identifiers*
>
> *9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:*
>
> *(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or*
>
> *(b) subclause 9.3 applies in relation to the adoption.*
>
> *Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.*
>
> *Use or disclosure of government related identifiers*
>
> *9.2 An organisation must not use or disclose a government related identifier of an individual unless:*
>
> *(a) 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 activities or functions; 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 required or authorised by or under an Australian law or a court/tribunal order; or*

[7] *JK and Department of Infrastructure and Transport* [2009] ADT 308 at [78].

> *(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or*
>
> *(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or*
>
> *(f) subclause 9.3 applies in relation to the use or disclosure.*
>
> *Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.*
>
> *Note 2: For permitted general situation, see section 16A.*
>
> *Regulations about adoption, use or disclosure*
>
> *9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:*
>
> *(a) the identifier is prescribed by the regulations; and*
>
> *(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and*
>
> *(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.*
>
> *Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).*

Previously, the restriction was to be found in the now repealed NPPs at Schedule 3 to the Privacy Act prior to 12 March 2014. NPP 7.2 provided:

> *7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:*
>
> *(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or*
>
> *(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or*
>
> *(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.*
>
> *Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).*

A private sector organisation that uses the DVS will breach APP 9.2 unless one of the exceptions apply. The most relevant exception to this PIA is APP 9.2(a) (which is the key difference from NPP 7.2 which informed the previous access policy) that is, *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 activities or functions.*

8.5 What is meant by "reasonably necessary" for the purposes of the organisation's activities or functions?

The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) (**Explanatory Memorandum**) provides the following guidance as to the meaning of the term "reasonably necessary":

> *A key objective of the Act is to balance the protection of the privacy of individuals, with the interests of public and private sector entities in carrying out their lawful and legitimate functions and activities*
>
> *The Bill also enables the personal information of an individual to be collected, used and disclosed in certain circumstances where it is `reasonably necessary' for one or more of the entity's functions or activities (agencies also have a `directly related' test) (APP 3 and 6).*
>
> *Key concepts - `reasonably necessary'*
>
> *A number of the APPs allow for collection, use or disclosure where the entity believes that the collection, use or disclosure is `reasonably necessary' for a particular purpose.* ***It is intended that this be interpreted objectively and in a practical sense****. It is not intended to provide a lower level of protection compared with the existing NPPs, where an objective test is implied*.
>
> *In relation to the requirement that an entity must not collect, use or disclose personal information unless it is reasonably necessary for a particular purpose, function or activity this is intended to reflect the following. The first is that the collection, use or* ***disclosure is reasonably necessary to pursue that particular purpose, function or activity. Whether the collection, use or disclosure is reasonably necessary is to be assessed from the perspective of a reasonable person (not merely from the perspective of the entity proposing to undertake the activity****).*
>
> *Where a reasonable person would not regard the purpose, function or activity in question as legitimate for that type of entity, the collection, use or disclosure of personal information will not be `reasonably necessary' even if the entity cannot effectively pursue that function or activity without collecting, using or disclosing the personal information.* [emphasis added]

The Explanatory Memorandum provides the following guidance in the context of APP 9

> *Since government related identifiers are generally highly reliable for verification and identification of individuals, their use and disclosure will be addressed by more specific guidelines than the general `use and disclosure' principle in APP 6.*
>
> *APP 9 will regulate the adoption, use or disclosure of government related identifiers by organisations.*
>
> *The principle will aim to* ***restrict general use of government related identifiers by the private sector so that government related identifiers do not become universal identifiers, as well as to prevent data-matching by organisations facilitated by the use and disclosure of those identifiers****.*
>
> *The principle will prohibit an organisation from adopting a government related identifier to identify an individual unless that adoption is required or authorised by or under law or allowed under the regulations. The principle will also prohibit an organisation from using or disclosing a government related identifier unless that use or disclosure falls within one of a list of specified exceptions. APP 9.2 will provide for exceptions relating to use or disclosure:*

> *where it is reasonably necessary to verify the identity of an individual for an organisation's activities or functions;*
>
> *These exceptions will recognise that balanced against the aims of the principle discussed above,* ***there may be circumstances where use or disclosure of a government related identifier by an organisation may be necessary for public purposes or present a clear benefit to the individual****. An example is to allow contracted service providers to use or disclose a government related identifier if necessary for the performance of a Commonwealth contract.*
>
> *The use of `reasonably necessary' in a number of the exceptions will ensure that an objective test is applied.*

In our view, the Explanatory Memorandum makes it clear that the new APPs are not necessarily intended to relax the restrictions on the use of government related identifiers and reflect public concerns that there not be any universal identifiers.

Whether disclosure is reasonably necessary is to be assessed from the perspective of a reasonable person and not from the perspective of the entity proposing to undertake the activity.

The OAIC has provided further guidance in the *Australian Privacy Principles guidelines* (February 2014), stating "*in the context of the Privacy Act, it would not be sufficient if the collection, use or disclosure is merely helpful, desirable or convenient*" [B.107]. The OAIC states at [B.108]:

> *The 'reasonably necessary' test is an objective test; whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of the APP entity to justify that the particular collection, use or disclosure is reasonably necessary.*

"Reasonably necessary" does not mean absolutely necessary but conduct consistent with what a reasonable and prudent person would do: *Thomas v Mowbray* (2007) 233 CLR 307; [2007] HCA 33at [23]. "Necessary" need not mean "*essential or indispensable, but … reasonably appropriate and adapted*": *Mulholland v Australian Electoral Commission* (2004) 209 ALR 582; [2004] HCA 41 at [39].

8.6 Legislative test for APP 9.2(a)

Having regard to the extrinsic material, the OAIC's guidance and case law, we consider that in order for a private sector organisation's use of the DVS to satisfy APP 9.2(a):

- the prospective user's activities or functions in question must be legitimate for that type of entity (assessed from the perspective of a reasonable person); and
- identification of an individual or being presented with the details of an evidence of identity document must be reasonably necessary for the prospective user's activities or functions (assessed from the perspective of a reasonable person); and
- verification of the evidence of identity document - that is, use of the DVS - must itself be reasonably necessary (assessed from the perspective of a reasonable person).

8.7 What types of private sector organisations may have a reasonable need to verify identity for the purposes of their activities or functions?

The first question is what types of private sector organisations would have a reasonable need to use the DVS within the terms of APP 9.2.

In every case, a user must satisfy the legislative test set out above.

In our view, if there is a requirement at law under any Commonwealth, State or Territory legislation to identify individuals then use of the DVS is likely to be reasonably necessary for the purposes of the organisation's activities or functions. In our view, a user who meets the existing access policy (described at 4.2 above) would meet the terms of APP 9.2(a) but a wider range of legislative requirements than superannuation, prepaid mobiles, banks, and financial transactions would also meet the terms of APP 9.2(a). If an organisation cannot lawfully perform its activities or functions without being satisfied of a person's identity, then its use or disclose a government related identity through a DVS check is likely to fall within APP 9.2(a).

If an organisation's activities or functions have a legislative role or purpose, then use of the DVS is likely to be reasonably necessary. An example of this would be the International English Language Testing System (**IELTS**) that has to check the identity of individuals sitting the test, particular IELTS scores being necessary to meet the legislative criteria for the grant of particular visas under the *Migration Regulations 1994* (Cth).

While most public safety obligations are legislated, we consider that if identification is for the purposes of protecting the public or a section of the public such as children or vulnerable persons, then use of the DVS may also be reasonably necessary for the purposes of the organisation's activities or functions. An example of this would be conducting background checks on foster carers or employees of aged care facilities. However, the legislative test under APP 9.2(a) must be met, including consideration of whether verifying the details of the evidence of identity document through a DVS check is reasonably necessary. If it would be enough to simply sight an evidence of identity document (for example, for the purposes of checking that a person is over 18 in order to serve him or her alcohol) then taking the further step of verifying the details through the DVS may not be reasonably necessary even though restricting alcohol from minors (for example) has an element of public protection. The key difference between sighting a document and verifying the details through the DVS is that agencies are involved in the DVS and must comply with the APPs.

It is not enough that using the DVS be convenient or efficient for a private sector organisation. Verifying identity is not likely to be reasonably necessary merely for the purposes of avoiding "bad debt". Organisations can seek payment in advance, can require a deposit, or build the risk that some individuals will not pay into the organisation's pricing structure.

We do not consider that APP 9.2(a) is restricted in its terms to a legislative requirement, particularly as legislative requirements is provided for in APP 9.2(c). We consider that where verifying identity is reasonably linked to the organisation's activities or functions, that is the activities or functions cannot reasonably be expected to be performed without knowing the identity of an individual, a private sector organisation would fall within APP 9.2.

A non-legislated code of conduct or voluntary industry scheme may require customer identification. This may bring members of that industry within APP 9.2, especially where there are consequences or sanctions for failing to comply with the code of conduct or voluntary industry scheme. However, the organisation's activities or functions in question must be legitimate and verification of the evidence of identity document must itself be reasonably necessary.

8.8 What types of private sector organisations should be permitted to verify identity for the purposes of their activities or functions?

The DVS should not facilitate a contravention of the APPs by users, nor by issuing agencies.

Accordingly, we recommend that there be clear, defensible criteria for assessing whether a prospective user falls within APP 9.2, in particular APP 9.2(a) that is whether using and/or disclosing government related identifiers is reasonably necessary for the organisation to verify the identity of individuals for the purposes of the prospective user's activities or functions. It is not enough that it be convenient or desirable, it must objectively be reasonably necessary. "Reasonably necessary" does not mean "absolutely necessary".

A clear access policy that would ensure that users who would not fall within APP 9.2 are not given access to the DVS could restrict access to the following circumstances:

a) the organisation cannot lawfully perform its legitimate functions or activities without verifying individuals' identity. A prospective user is likely to fall within APP 9.2 if there is a Commonwealth, State, Territory or local government requirement that the prospective user know who their customer is.

b) the organisation has specific obligations to an agency or a State or Territory authority to verify identity.

c) the prospective user has a responsibility to protect the public or some section of the public, and identification is reasonably necessary for that activity or function.

d) it would not be reasonable to expect an organisation to perform its legitimate functions or activities without verifying individuals' identity.

In our view, a private sector organisation that satisfied such a policy would be likely to meet the requirements of APP 9.2.

We note that the policy could legitimately specify classes of organisations that would meet the policy requirements, or provide that organisations with particular characteristics or functions would ordinarily meet the policy. We also note that there is no legal obligation to give DVS access to any organisation.

9. Other privacy risks

9.1 Community views

The OAIC *Community Attitudes to Privacy Survey Research Report* 2013 indicates that the community:

e) is concerned about the risk of identity fraud and identity theft;

f) is unhappy with their personal information being sent offshore;

g) does not like their activities being monitored on the internet

h) trusts government entities more than private enterprises, with the exception of health organisations and financial institutions;

i) expects high standards of transparency in data handling and thinks that organisations should inform them how their personal information will be handled and protected, and should inform them if their personal information is lost; and

j) considers that scanning identification documents is acceptable in order to obtain a credit card but is unacceptable in relation to everyday activities, even where proof of age is required such as entry to licensed premises, buying alcohol and buying cigarettes. 95% believe scanning identification in relation to purchases of general goods is unacceptable.

One of the relevant principles identified by a consumer advocacy group was consumers should have accessible and effective remedies for failures and breaches of the law.

Having regard to the OAIC survey and to the feedback we received in consultation, we have summarised other privacy risks in the table below: **Privacy risks**

Although the DVS is more protective of personal privacy than many existing methods of identification currently used by private sector organisations, the existing methods are not sanctioned or facilitated by government. In relation to expanded private sector access, the DVS should not facilitate a contravention of APP 9 by users who would not fall within APP 9.2.

In the context of wider private sector access, smaller organisations may not have the same resources in terms of privacy compliance and information security.

Consumers are likely to be uncomfortable with widespread use of the DVS or use of the DVS where the need to verify identity documents is not obvious.

People have a right to be anonymous in most situations. Requiring evidence of identity should not be automatic.

There may be negative consequences arising from an 'N' response. The individual is not a party to the agreement between the user and the AGD and may not know how to address the problem.

The greater the number of users, the greater the risk of misuse of the DVS, and the greater the risk of information being used for a secondary purpose.

We have taken these risks into account and consider that these risks will be adequately addressed by our recommendations in section 3 above, having regard to the existing arrangements.

Schedule 1 - Glossary

AGD	The Commonwealth Attorney-General's Department
APP	Australian Privacy Principle
ATO	Australian Taxation Office
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Human Services
DVS Hub	The component of the DVS infrastructure that connects document issuing agencies and users/GSPs and allows for DVS match requests and responses to be securely routed between them
EOI	Evidence of Identity
FSM	Field Specific Matching, that is a response to a DVS query that indicates which of the fields did not match the records of the issuing agency
GSP/Gateway Service Provider	A Gateway Service Provider allows approved private sector and government users to interrogate the DVS through the Gateway Service Provider's interface. The GSP provides the channel through which users access the DVS or are authorised to access the DVS on behalf of a user who requires the identifying information to be matched
NPP	National Privacy Principle (now repealed)
OAIC	The Office of the Australian Information Commissioner
PIA	Privacy impact assessment
Privacy Act	The *Privacy Act 1988* (Cth) as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) with effect from 12 March 2014
User	A government agency or private sector organisation who uses the DVS to verify records against the issuing agency's records, either through direct access to the DVS through their own DVS interface or by using the services of a Gateway Service Provider

Schedule 2 - Documents considered in the course of the PIA

Background information

4. The information contained on the DVS website: www.dvs.gov.au

5. The information contained on the DVS page of the AGD website: http://www.ag.gov.au/rightsandprotections/identitysecurity/pages/documentverificationservice.aspx

6. *Document Verification Service: An Overview* (V4 December 2013)

7. *DVS Data Flow and Storage* flowchart

8. National Identity Security Coordination Group 23 November 2011 Item 4b

9. DVS Advisory Board 2 December 2013 Item 8

10. *Document Verification Service: Private Sector Access National Service Offering Industry Briefing Note* May 2013

Relevant policies

11. DVS Access Management policy: A policy for access to the Document Verification Service by Business Users

12. Document Verification Service An Overview for Private Sector Use V2.2 July 2013

Contractual documents

13. Document Verification Service: Gateway Service Provider Application Form and attached Document Verification Service Gateway Service Provider Terms and Conditions of Use

14. Document Verification Service: Business User Application Form and attached Document Verification Service Business User Terms and Conditions of Use

15. Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013

16. Document Verification Service Supporting Material - Module 3 Interface Definitions version 9 November 2013

17. Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013

Existing privacy impact assessments

18. Attorney-General's Department Cyber and Identity Security draft paper entitled Application of the APPs

19. Attorney-General's Department Privacy Impact Assessment: National Document Verification Service June 2007

20. Information Integrity Systems Draft Preliminary Privacy Assessment: Information Brokers Access to the Document Verification Service 17 July 2012

21. Information Integrity Systems Extension of Document Verification Service to Private Sector Organisations 20 July 2012

Document Verification Service - expanded private sector access, Privacy Impact Assessment

Previous audits conducted by OAIC and its predecessor the Office of the Privacy Commissioner

22. National Document Verification Service, Department of Foreign Affairs and Trade, Department of Immigration and Citizenship, ACT Department of Births Deaths and Marriages, ACT Road User Services, Centrelink May 2009

23. National Document Verification Service, Department of Immigration and Citizenship - Audit Report March 2010

24. National Document Verification Service, Attorney-General's Department Final Audit Report May 2010

25. National Document Verification Service, Centrelink - Audit Report June 2011

26. National Document Verification Service - Department of Foreign Affairs and Trade - Audit Report December 2012

Schedule 3 - State and Territory Agencies and legislation

The following State and Territory agencies allow the DVS to verify the details of documents, save that only government agencies are able to verify Births Deaths and Marriages documents pending a review of access to CertValid):

a) New South Wales:

I. Attorney General & Justice - Registry of Births, Deaths & Marriages (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - *Births, Deaths and Marriages Registration Act 1995* (NSW);

II. Roads and Maritime Services (driver licences) - *Road Transport (Driver Licensing) Act 1998* (NSW);

b) Victoria:

I. Department of Justice - Births, Deaths & Marriages (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act 1996 (VIC);

II. State Revenue Office (VicRoads) (driver licences) - Road Safety Act 1986 (VIC);

c) Queensland:

III. Department of Justice and Attorney-General - Births, Deaths and Marriages (birth certificates, change of name certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act 2003 (QLD);

IV. Department of Transport and Main Roads (driver licences) - Transport Operations (Road Use Management) Act 1995 (QLD);

d) South Australia:

V. Attorney-General's Department - Births, Deaths and Marriages Registration Office (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act 1996 (SA);

VI. Department of Planning, Transport and Infrastructure - Motoring (driver licences) - Motor Vehicles Act 1959 (SA);

e) Western Australia:

VII. Department of the Attorney General - Registry of Births, Deaths & Marriages (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act 1998 (WA);

VIII. Department of Transport - Driver and Vehicle Services (driver licences) - Road Traffic Act 1974 (WA);

f) Tasmania:

IX. Department of Justice - Births, Deaths and Marriages (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act 1999 (TAS);

X. Department of Infrastructure, Energy and Resources - Transport (driver licences) - Vehicle and Traffic Act 1999 (Tas);

g) Australian Capital Territory:

XI. Office of Regulatory Services - Births, Deaths and Marriages (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act 1997 (ACT);

XII. Territory and Municipal Services (driver licences) - Road Transport (Driver Licensing) Act 1999 (ACT).

h) Northern Territory:

XIII. Department of the Attorney-General and Justice - Births, Deaths and Marriages (birth certificates, change of name certificates, marriage certificates) (not presently available to checks by private sector users) - Births, Deaths and Marriages Registration Act (NT);

XIV. Department of Transport - Motor Vehicle Registry (driver licences) -Motor Vehicles Act 1949 (NT).

We have not considered compliance with State and Territory privacy legislation but note that it would include (but is not limited to) the following:

i) New South Wales: Privacy and Personal Information Protection Act 1998 (NSW);

j) Victoria: Information Privacy Act 2000 (VIC);

k) Queensland: Information Privacy Act 2009 (QLD);

l) South Australia: Information Privacy Principles Instruction (SA);

m) Western Australia: Freedom of Information Act 1992 (WA) and various agency-specific provisions;

n) Tasmania: Personal Information Protection Act 2004 (TAS);

o) Australian Capital Territory: Privacy Act 1988 (Cth); and

p) Northern Territory: Information Act (NT).

Schedule 4 - Contractual requirements

Defined terms in this Schedule are defined terms found in the Document Verification Service Business User Terms and Conditions of Use (**Attachment 2**) and Document Verification Service Gateway Service Provider Terms and Conditions of Use (**Attachment 3**).

1. DVS Business User Terms and Conditions of Use

Pursuant to the DVS Business User Terms and Conditions of Use (**Attachment 2**), a user must itself be an approved GSP or have in place an arrangement with a third party currently approved GSP: clause 2.2.

Users are required to strictly comply with all instructions and guidance provided by AGD: clause 7.

1.1 Secondary purpose

Except as may be specifically advised in writing by the AGD, users must not access or use the DVS for any purpose other than for the purposes of meeting statutory obligations in relation to identity verification (clause 8.1) and must not allow any person other than authorised personnel to access or use information match data or the DVS Business User ID (clause 8.3). Personal information obtained through use of the DVS must not be used for any purpose other than access to and use of the DVS: clause 8.5.

1.2 Privacy

Clause 11 of the DVS Business User Terms and Conditions of Use provides that "*You must ensure that your use of the DVS and Information Match Data complies with the Privacy Act 1988*".

Users must have a privacy policy (which must be attached to the Business User Application Form at **Attachment 3**), must comply with that policy and must not make any change to that policy without giving the AGD at least 30 days' notice in writing: clause 13.

1.3 Consent

DVS checks must be undertaken with the informed consent of the person whose information is being used. An individual providing their document details for verification must be "*informed of the purpose for which that information is sought and will be used by you (including that the information will be subject to an Information Match Request in relation to relevant Official Record Holder information, and that a corresponding Information Match Result will be provided via the use of third party systems*" (clause 12.2.) and must provide "*their express consent for such use and accessing such information prior to any such use or access being initiated or made by you*" (clause 12.3). However, users must not make any public statement concerning their access to the DVS or their use of the DVS: clause 8.6.

1.4 Auditing

Users and their GSPs must fully cooperate with any audit or verification process checking their compliance, including providing access to premises, facilities, systems and records: clause 10. DVS Information Match Responses must be recorded so that compliance with the Conditions can be audited: clause 2.4.

1.5 Security

Users must comply with all security procedures advised by the AGD and take all reasonable action to maintain the security of the DVS including maintaining the security of tokens, access codes, and encryption keys (clause 16) and must take all reasonable action to prevent and detect unauthorised use of the DVS or their Business Access Systems (clause 18). Users

must immediately notify the AGD of any suspected compromise of security information, unauthorised use or security breach (clause 18).

Users and GSPs can be suspended at any time for any reason (clause 24) and users can be terminated immediately for breach of the DVS Business User Terms and Conditions of Use (clause 25.2).

2. Gateway Service Provider Terms and Conditions of Use

2.1 Access

Pursuant to the Gateway Service Provider Terms and Conditions of Use (**Attachment 3**), GSPs cannot connect to the DVS and provide Gateway Services until the Gateway System has been fully tested and is compliant with the AGD's Gateway System certification requirements: clause 2.

GSPs are required to strictly comply with all instructions and guidance provided by the AGD: clause 10.

GSPs can only accept Authorised Business Users as Gateway Users who must be required to comply with the DVS Business User Terms and Conditions of Use: clauses 3 and 4. GSPs may not themselves make an Information Match Request unless they are also an Authorised Business User: clause 11.6.

GSPs must fully cooperate with any audit or verification process checking their compliance, including providing access to premises, facilities, systems and records: clause 13.

2.2 Security

GSPs must comply with all security procedures advised by the AGD and take all reasonable action to maintain the security of the DVS including maintaining the security of tokens, access codes, and encryption keys (clause 17) and must take all reasonable action to prevent and detect unauthorised use of the DVS or their Gateway Systems or Gateway Services (clause 18). Users must immediately notify the AGD of any suspected compromise of security information, unauthorised use or security breach (clause 19).

2.3 Privacy

GSPs must have a privacy policy (which must be attached the Gateway Services Agreement Form at **Attachment 3**), must comply with that policy and must not make any change to that policy without giving the AGD at least 30 days' notice in writing: subclauses 14.3 and 14.4.

Except as specifically authorised by the AGD in writing, GSPs must not collect or store Information Match Results: clause 11.5.

2.4 Consent

GSPs must ensure that the individual whose document details are being checked has provided his or her prior informed consent: clause 14.1.

3. DVS Supporting Materials

We understand that the instructions and guidance provided by the AGD (that GSPs must comply with pursuant to clause 10 of the Gateway Service Provider Terms and Conditions of Use, and users must comply with pursuant to clause 7 of the Business User Terms and Conditions of Use) currently include in the DVS Supporting Materials that are provided to GSPs.

The Supporting Materials provide that "*Access to the DVS will be for the sole purpose of confirming the integrity of identifying information provided by an individual as evidence of*

identity (EOI)": Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at section 4.5.

We note that the Document Verification Service *An Overview for Private Sector Use* V2.2 July 2013 provides that "*A positive or negative response received through the DVS may not be used as the sole basis for a decision to enrol or not enrol an individual for benefits or services*."

Users and GSPs are required to submit annual (or more frequent) compliance statements which must, at a minimum, confirm that the user's (or GSP's) use of the DVS is in accordance with the Terms and Conditions of Use and the DVS Supporting Material or, if the user did not fully comply with the Terms and Conditions of Use and DVS Supporting Material, what actions have been or are being taken to address the contravention: Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at sections 4.7 and 4.8.

GSPs are audited annually by independent auditors for compliance with the DVS terms and conditions (most users accessing the DVS through a GSP). GSPs either conduct the electronic search on behalf of the user or provide the customer identification service through which they are responsible for obtaining the details of the identity document and the individual's consent to the DVS check. Users are audited on the basis of risks identified in assessing compliance statements: Document Verification Service Supporting Material - Module 1 Business Requirements version 9 November 2013 at section 4.7.

3.1 **Security**

The DVS Supporting Materials with which users must comply include extensive security requirements: Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013; see also *Document Verification Service: An Overview* (V4 December 2013).

The DVS Hub allows requests and responses to be securely routed between users (or GSPs) and agencies. The DVS Hub has a number of security features including firewall and environment security, intelligent message transformation and routing and management information and audit logs.

DVS security policy is based on the Australian Government Protective Security Policy Framework (PSPF), the technology control minimum standards specified in the Australian Government Information Security Manual, and relevant Australian and New Zealand IT Security standards.

All user and GSP personnel who perform DVS ICT administrative or system functions must be employment screened in accordance with PSPF level 1 (government agencies) or with the Australian Standards AS4811:2006 – Employment Screening (private sector organisations).

Users and GSPs are required to log activity and transactional data to enable monitoring for and reporting of security breaches. Users, GSPs and issuing agencies are required to report security incidents or information security events to the DVS Operations Manager and the DVS Manager. Security incidents that must be reported include (but are not limited to):

- DVS targeted emails with attachments or links;
- any compromise or corruption of DVS information;
- unauthorised access or intrusion into a DVS ICT system;
- DVS data spills;
- introduction of viruses/malware to a network with DVS operations;

- theft or loss of electronic devices that have access to DVS systems or have processed or stored DVS data;
- evidence of attempted trawling;
- Denial of Service attacks directed to DVS Internet based services; or
- suspicious or unauthorised network activity.

DVS Participants must have a designated Security Incident Investigator responsible for notifying the DVS Hub Security Incident Investigator and DVS Manager of any DVS security incidents. The DVS Hub Security Investigator will then report on the incident to the DVS Manager who will subsequently advise the National DVS Advisory Board: see Document Verification Service Supporting Material - Module 6 Security Plan version 9 November 2013.

Security incidents may also be reported to appropriate external parties (such as the police or the OAIC).

Schedule 5 Summary of responses received during consultation process

Summary of expanded access privacy risks and benefits identified by issuing agencies

The following privacy risks, benefits and mitigating measures in relation to expanded access were identified by **issuing agencies**:

Privacy positives	False identities enable very serious crimes (including people trafficking) and is a threat to national security. The DVS is a critical national asset in the fight against identity theft. Expanded commercial access is in keeping with government and community commitment to eliminating or reducing identity theft and promoting a safer community and commercial environment. The DVS is safer than other mechanisms for checking veracity of government documents with fewer or no accountability mechanisms and safeguards, less recourse to copying documents. A high correlation is anticipated between improvements in identity security through use of the DVS validation availability to a broader range of organisations, and the reduction of identity fraud. There are benefits to the entire community from the DVS. In general, expanded private sector use of the DVS could be a good thing because if documents are checked then fake documents are less lucrative. There are many privacy benefits from the DVS. It is a good quality product, and is far better than holding a photocopy. Life without the DVS would mean weaker identity security and more identity theft.
Privacy risks	Potential 'N' responses for individuals will not be explained, i.e. whether it was a data entry error, expired documentation used, or fraudulent document. The 'N' response is expected to negatively impact an individual whose identity is being verified by an organisation. The negative impact may include financial and legal implications for the individual, and while unlikely, it may lead to prospective legal liabilities for the DVS and issuers. We are moving more and more into digital age and the DVS may not be solution. What else is out there? Opening access to the data to anyone increases the risk that there has not been consent from the data owner. Medicare card-holders may not be aware that their card is used for another purpose (identity verification). Medicare cards are not as high-security as other documents (for example, newborn babies can be registered from home).
Measures to mitigate the risk	Existing security and access controls must apply to expanded access. Legislative sanctions required for breaches, not just contractual.

Summary of expanded access privacy risks and benefits identified by users

The following privacy risks, benefits and mitigating measures in relation to expanded access were identified by **users and GSPs**:

Privacy positives	Other methods of identity verification such as paper-based verification (which requires copying of identity documents), digital imaging of ID documents online, customer transaction history and screen-scraping (using a customer's details to access a third party database which raises particular privacy concerns) are more privacy-intrusive. Screen-scraping uses Medicare, Passports, driver licence and electoral roll websites, web-harvesting trawls the internet with a crawler for information on a person, web-transacting on Google and Facebook, 100 point system. The DVS is far better from a privacy perspective. The DVS protects privacy much better than existing methods which are informal and without strict controls such as web-transacting, web-harvesting, screen-scraping. The DVS has much better controls and structures. The DVS protects privacy far more than paper based methods with documents photocopied, posted - these methods are privacy intrusive and lack controls and consistency. DVS use means less of a need to retain copies of an individual's identification documents and therefore a lower risk of a data breach. The DVS enhances timely provision of products and services to the consumer's benefit. Online enrolment is key to digital services online, the DVS would have a critical role in online identification through official channels in an accurate way. This would be a real positive for the Australian economy, and promote trust and confidence in the digital economy. The DVS safer for privacy e.g. you can remove an operator's access, but you can't do that with a hard copy licence sitting around The DVS reduces the amount of information a person has to reveal, it is light touch, high certainty and involves no disclosure. Manual production/collection of documents is cumbersome, unreliable and more privacy intrusive. A log noting "match achieved" is kept versus a photocopy with more information. Less information is revealed through the DVS - only the details necessary to obtain a match (as opposed to a copy of a driver's licence which reveals whether an individual wears glasses, or is an organ donor). The DVS should be more widely available on the grounds of protection of privacy and in the interests of consumers. The current restriction to a legislative requirement is artificial and undesirable. The DVS enhances privacy as no print-outs lying around, there are log-in controls and it is secure. Current methods of verifying identity (documents, certified copies, all your details in a filing cabinet with a 50 cent key) are unregulated and carried out by unskilled people, they are a big source of breaches and latent breaches of privacy

Privacy risks	The DVS is a very effective service for a specific purpose but if it is extended where it doesn't need to go it undermines the service. The DVS's value lies in its effectiveness and limited access to it, we don't want customers to see the DVS "as some creepy thing". Banks and Telco's need to know their customer but a liquor store or nightclub has no need to verify it. The AGD should limit use of the DVS to where there is a clear need. Smaller organisations are accumulating more and more personal information but there has not been a corresponding investment in information security or privacy compliance. A small organisation can have a large breach. Data breaches have a flow-on effect on the economy. The DVS needs clarity around access, which should be a reasonable need to verify identity, and subject to APPs
Measures to mitigate the risk	The DVS needs security and access controls to prevent misuse, such as a legislated requirement for specific security standards and dedicated privacy and security personnel to use DVS, enforced standards, controls (including access abuse monitoring) and audits. Individuals need to know how their identity information is being used or stored. "reasonably necessary" - the DVS is a real positive in the move towards an online economy but should be some form of legislative requirement to gain access. The DVS is not the answer to all aspects of the online economy or the solution to online trading, the point of PayPal was to be able to transact anonymously. In most cases it is enough to be paid in advance, with no need to check a driver's licence. There is a risk of data breaches, users must have excellent security with an end to end security process and PIA. Smaller organisations do not have the same resources for IT security and do not necessarily have the commitment. There should be mandatory information security standards or published guidelines. There should be a Data Breach Policy and Employee Data Breach Policy with legal and compliance consequences, contractual not legislated GSPs have compliance statements and audits, and are a safe way for smaller users to have access to DVS. Give access to larger organisations used to handling mass data rather than to newsagents (for example). Consent is not real consent if you are not given an option. Should be clear alternatives such as coming in person at no additional cost, or going elsewhere Reporting data breaches should be mandatory. There should be crystal clear legislative obligations and consequences, perhaps federal legislation for the DVS. If a wider range of entities has access to the DVS, there needs to be strict controls and observable obligations. GSPs play an essential role in safeguarding privacy. GSPs have interface protocols, can turn DVS matches into something useable for AML-CTF, and can provide an integrated layer of services.

Summary of expanded access privacy risks and benefits identified by other entities

The following privacy risks, benefits and mitigating measures in relation to expanded access were identified by **privacy groups**:

Privacy positives	The DVS reduces the need for hard copies. There are genuine consumer benefits in DVS if used properly, a national security efficiency dividend and consumer benefits. The DVS can be a real benefit. No issue with current Y/N responses.
Privacy risks	Opening up a broader spectrum of users increases the risk of function creep. Documents were never intended to have that purpose, especially the Medicare card. Documents are not presented by the individual - may be by phone, keyed into online system, or simply transferred from the requesting agency's own system. "Yes" does not mean document has been verified, "No" does not mean the document itself is false. The DVS is not a consent based system as consent is not freely given when individuals are required to provide information to obtain a service or benefit. The DVS will not often be necessary. Utilities know where you live to deliver power and, so long as you pay, don't need to verify your identity. A rental car company just needs to see your licence not verify it. The more organisations with access and the more fields matched, the greater the privacy risks. The absence of governing legislation for the DVS means there is no protection for individuals, who are not a party to the contract or MOU. Increases the risk of misuse, especially if combined with FSM.

Measures to mitigate the risk	Users must be covered by the APPs - opt-in principle. There should be a contractual requirement so that if exempt from the Privacy Act the user has opted in. There needs to be a high degree of openness. There must be a prohibition on secondary uses, e.g. verify document for that primary purpose only. APP 1.4 - users should have privacy policies addressing how personal information is to be used. There needs to be strict limitations on "repurposing" of data, "function creep". There should be a legislative requirement to give reasons for refusing an application based on a DVS non-match. Legislation should require disclosure of certain information about the nature of the DVS to consumers. Social media and internet should not get access - individuals must be free to be anonymous or use an alternative identity online. Flybuys and Everyday Rewards should not get access. There must be informed consent with a notification which is in plain English, readable, and upfront regarding any other options. A good example is the standardised Telco's critical information summary which allows individuals to see at a glance what happens with the information and who it's shared with. The existing principles for access are appropriate set of minimum requirements. There needs to be clear notification to individual at the outset - this will be used to verify your identity, why the information is provided, and how it will be used. The DVS Access and Management Policy will need to explain what is meant by "reasonably necessary" with the onus on the applicant to satisfy the Committee of the reasonable need. The smaller the amount of users with the best security, the safer from a privacy perspective, if there is wider use there needs to be strong safeguards. Users must all comply with APP 5 and also generally explain to individuals what they are consenting to (give them notice of what will be done if they wish to proceed with the transaction), be consumer friendly. The terms and conditions should include the APPs so that users who are exempt from the Privacy Act are still bound by the APPs. The terms and conditions should make it crystal clear that information can't be used for a secondary purpose, this should be monitored. The DVS needs to be fully consent based with the individual aware of the disclosure from the user to the DVS hub to the agency to the DVS hub to the user, with these disclosures and uses to be conducted within the APP guidelines There needs to be an explicit channels for appeals/challenges to adverse conclusions. Agencies and commercial entities should be obliged to set out the information used and the reasons for decision, individuals must be informed of the nature of adverse information. Protection of hard copy and electronic data should be to at least standard of logical and physical security as Australian Government - locked, controlled access. There need to be compliance audits and public reporting of deficiencies. Good information security practices are needed. There should be a legislative requirement not to keep logs or data trails longer than a specified period of days. Access should only be given to closely regulated sectors e.g. banks and Telco's which are more serious about privacy. GSPs have a role to play.

Summary of other comments

What is meant by "reasonably necessary"?	"Reasonably necessary" is an objective test, could the organisation perform the function/services without identifying or identifying in another way than a government identifier. APP 9.2 uses the concept of "need" not "want" - it cannot be merely useful or convenient.
What types of organisations might seek access?	Potentially anyone might ask for access - even dating websites (see for example EHarmony and RelyID), proof of age for liquor. The real estate industry needs to know the identity of purchasers and tenants - it currently uses paper-based standard for EOIs. Utility providers will benefit - have to have "acceptable" identification under National Energy Retail Rules, suffer from bad debt.
What types of organisations should get access?	Telco's, utilities companies, real estate, sensitive employment environments, universities, registration of health professionals, criminal checks. "reasonably necessary" - maritime and aviation security screening, screening employees for access, State and Territory obligations such as second hand goods, FTRA supports State obligations, real estate, car rentals, car share, hotel safety deposit box, gaming machines, child protection, personnel screening agencies. As to who has a reasonable necessity: new electronic conveyancing laws require verification of documents, without DVS no way of verifying documents, only paper-based process. Real estate agents, lawyers, bankers will need to use DVS. Real estate agents also need to know who the tenants are. There needs to be a clear public interest justification. There should be a robust process of use so only organisations with a sophisticated understanding of identity verification gain access to the DVS. GSPs may have a role here. Also, the government has insufficient resources to audit everyone. There should be clear, defensible criteria for access to DVS and if an organisations meets the criteria it should get access, if not then no access. If there is a legislative requirement then there ought to be access. If there exists a regulatory obligation to know identity at any level of federal, State or local government then the DVS should be available. The test should be whether the organisation is obligated to know the identity, some kind of regulatory requirement, and the organisation should fall under the Privacy Act. The fact that the amended Privacy Act may allow greater use does not mean that the Government is obliged to facilitate greater use.

General comments	Consumer interest groups should be consulted. NGOs consulted should include a wider group e.g. ACCAN, CFA and Choice to capture what it means from consumer perspective. A wider range of advocacy organisations need to be consulted e.g. financial, telecommunications and consumer fields especially credit sector given *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. There should be a consumer representative on the DVS Advisory Board or Steering Committee. The world is moving online without branches or stores. The DVS is critical to the online economy. The online economy can't have 2 streams: the fast lane for those who can use the DVS, the slow lane for those stuck on paper-based systems. Regarding multiple identities: • The DVS should accommodate legitimate use of different identities in different circumstances, often necessary (witnesses, abuse victims); and • It is not unlawful to use different names in different contexts. The more centralised the checking system, the more disparities are apparent. DVD needs explicit reminders that a non-match need not be adverse and remind users of obligations under APPs especially APP 5; versus • The DVS doesn't prevent multiple identities - the individual knows who they are in a particular context; and • The DVS does not change the risk for abusive women (for example). People use different names but they know who they are in a particular context - e.g. NSW Driver Licence will record my name as X. A mismatch or failure to verify need not be grounds for suspicion or adverse action. Will the DVS remain in government or be privatised? Privacy pluses to use by a few trusted gateway services providers not smaller businesses. How will it impact upon the AML-CTF credit reporting? The fact that the amended Act may allow wider use does not mean that the government is obliged to facilitate it. There needs to be a clarity of objectives as to why DVS should facilitate industry in this way. The use of a digital identity safeguarded by a bank or the government as an identity provider such as the USA National Centre for Trusted Identities in Cyberspace is an alternative solution to the digital economy, the UK and NZ are moving that way. Hard evidence and systemic reasoning is needed to justify privacy invasive aspects needed - defined objectives, empirical costs of volumes and financial benefits. The mere fact that privacy protections have been weakened need not mean that government has to loosen constraints (or "grease the wheels of commerce"). It is vital that the need for multiple identities be explicitly recognised. Other than passports, the documents are not identity credentials - they attest to an attribute of an individual (a visa, permission to drive). Data is not disclosed for the purpose for which is was collected. "Yes" does not mean document has been verified, "No" does not mean the document itself is false. The DVS is not a consent based system as consent is not freely given when individuals are required to provide the information to obtain a service or benefit. Medicare should have its own PIA as it represents a new use completely unrelated to the purpose of the card and the Medicare database is unreliable.

Attachment 1 - Invitation to comment

Document verification service

Consultation paper for privacy impact assessments for proposals to enhance the document verification service

22 January 2013

Request for assistance from AGD

The Australian Government Attorney-General's Department (AGD) has commissioned Clayton Utz to prepare reports scoping the potential privacy impacts of proposals to enhance the availability and functionality of the national Document Verification Service (DVS) in terms of recent Commonwealth privacy reforms. The proposals involve both privacy risks and benefits. To develop the privacy impact assessments, AGD seeks your assistance in identifying these risks and benefits, as well as potential controls or mitigation strategies.

To this end, AGD has asked Clayton Utz to conduct targeted consultation with key stakeholders related to the Commonwealth components of the service. This paper is intended to provide a brief overview of the proposals to assist in the consultation process.

The consultation process, and how you can assist, is set out in the next steps section of this paper (on page 5).

Contents

Background—What is the DVS?

AGD manages the DVS on behalf of all Australian governments. The DVS is a key element of the National Identity Security Strategy endorsed by the Council of Australian Governments.

The DVS is a secure online system that enables organisations to verify information on a customer's evidence of identity documents with the records of the document issuing agency.

The DVS currently provides organisations with the ability to verify information on a range of evidence of identity documents issued by Australian Government and state and territory government agencies. These include immigration documents, passports, driver licenses, Medicare cards as well as birth, marriage, and change-of-name certificates.

The DVS is not a database. DVS transactions involve a check of whether the information presented on an evidence of identity document matches the records of the issuing agency. The results are provided in the form of a 'yes/no' result. DVS checks must be undertaken with the informed consent of the person whose information is being used, and no personal information is retained following the completion of a check.

DVS checks have been available to by government agencies since 2009, and
(with the exception of birth, marriage and change of name data) are now being made available to the private sector, with an initial focus on organisations that have legislative obligations to identity their customers. For example, financial institutions which need to meet 'know your customer' requirements in anti-money laundering and counter-terrorism financing regulations.

Any organisation using the DVS is required to comply with the *Privacy Act 1988* (Cth) or any relevant state and territory privacy legislation.

For further information on the DVS see www.dvs.gov.au.

Proposals to expand the functionality and availability of the DVS

AGD is considering two proposals which are set out below. In addition, some of the privacy risks and benefits which have already been identified are set out.

<table>
<tr><td rowspan="2">1</td><td>Expanded commercial access: Reforms to the Privacy Act 1988 will come into effect in March 2014 which include amendments to use by organisations of Commonwealth government identifiers (previously dealt with by NPP 7.2). The new APP 9.2 allows use of government identifiers by organisations in different circumstances, including where '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 activities or functions.'
The current DVS access management policy (see the Attachment at page 6) limits commercial access and use to businesses operating under legislated client identification requirements. This restriction was informed by the prohibitions and permissions of the Privacy Act 1988 (NPPs 7.2, 2.1). In light of privacy reforms AGD is reviewing DVS access policies and is considering in particular potential privacy risks in expanding the range of businesses eligible for DVS access as may be permitted under the APPs.</td></tr>
<tr><td>Potential privacy issues, risks and benefits:
• Defining the circumstances in which use of an identifier is "reasonably necessary" for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions
• Facilitating online transactions without the need for hardcopy identity documents to be provided
• Limiting use by organisations to circumstances only where there is a reasonable need to verify the identity of the individual for the organisation's activities or functions
• Avoiding more intrusive identity verification methods, for example avoiding the need for organisations to keep copies of identity documents</td></tr>
<tr><td rowspan="2">2</td><td>Expanded functionality (field specific matching): DVS technical functionality currently provides a one character response indicating the cumulative accuracy of all data fields used to match a document – a confirmed match (Y) response indicates that all five fields completely match. Negative responses provide no information as to why an N result is returned.
The challenge of translating the complexity of some identity documents into DVS match requests can result in inaccuracy at the data entry stage and the return of false 'N' responses. This can result in Users resubmitting queries until a Y result is returned, generating multiple unnecessary N results and additional traffic through the system.
Field specific matching (FSM) could assist Users to minimise the number of repeat match requests by providing a code from the Issuer indicating formatting errors or fields that were not matched in the search. Both public and private sector Users have indicated a strong interest in such a capacity.
An FSM code would simply refer the User back to a specific field on the identity document for re-examination. AGD anticipates that FSM could deliver considerable service improvements to organisations and their customers by limiting the degree of guesswork in DVS requests, reducing the amount of retried queries, minimising the time taken to gain an accurate result, and improving customer service.</td></tr>
<tr><td>Potential privacy risks and benefits:
• Avoid unnecessary false negatives due to input error
• Improve identity decision-making by providing Users with information to start a discussion with a customer
• FSM could reduce the amount of information which is necessary for the purposes of verifying an identity
• Whether there are other ways in which false negatives could be avoided without FSM</td></tr>
</table>

Privacy impact assessments into the proposals

AGD has instructed Clayton Utz to prepare two privacy impact assessments in relation to the two proposals discussed.

► Report A—Privacy impact assessment of expanded private sector access

We are instructed to prepare a Privacy Impact Assessment (PIA) identifying privacy impacts and options to mitigate any privacy risks related to extending use of the DVS to private sector organisations in the context of the national privacy regime set out in the *Privacy Act 1988*, as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

Report A will:

5) assess the privacy risks associated with expanding the range of businesses able to use the DVS for the purposes of verifying information on government issued identifiers to include any organisation with a 'reasonable necessity' to identify an individual as per Australian Privacy Principle (APP) 9.2(a)

6) assess any privacy benefits that may accrue from wider private sector use of the DVS, as an alternative to other methods of verifying government issued identifiers that are commonly used by private sector organisations, and

7) identify options to mitigate any privacy risks associated with expanded private sector use of the DVS.

In doing so the report will need to take into account:

- the draft PIA material prepared by AGD
- existing privacy and information security measures including contractual terms and conditions on DVS private sector access; existing privacy, information security, and business rules of the DVS, and
- governance processes for DVS private sector access.

Preparation of the report will include consultations with a range of Commonwealth government and non-government stakeholders such as:

- Commonwealth document issuing authorities – Department of Foreign Affairs and Trade, Department of Immigration and Border Protection, Department of Human Services;
- DVS User organisations – government and business;
- The Office of the Australian Information Commissioner – the Privacy Commissioner, and
- Non-government privacy advocates (Australian Privacy Foundation, Liberty Victoria, Electronic Frontiers Australia)

Report B—Privacy Impact Assessment of Enhanced DVS Functionality (field specific responses)

We are instructed to prepare a Privacy Impact Assessment identifying privacy impacts and options to mitigate any privacy risks related to enhancing the DVS to return responses indicating the specific data field(s) that did or did not verify. The report will consider these impacts in the context of the proposed expansion of DVS private sector access (Report A).

Report B will:

4) assess the privacy risks associated with the enhanced DVS functionality providing data field specific responses,

5) assess the privacy benefits associated with enhanced DVS functionality, and

6) identify options to mitigate any privacy risks associated with the enhanced DVS functionality.

In doing so the report will need to take into account:

- Report A: Privacy Impact Assessment of Expanded Private Sector Access
- draft business model material prepared by AGD
- existing privacy and information security measures including contractual terms and conditions on DVS private sector access, existing privacy, information security, and business rules of the DVS, and
- governance processes for DVS private sector access.

Preparation of the report will include consultations with a range of Commonwealth government and non-government stakeholders such as:

- Commonwealth document issuing authorities – Department of Foreign Affairs and Trade, Department of Immigration and Border Protection, Department of Human Services
- DVS User organisations – government and business
- The Office of the Australian Information Commissioner – the Privacy Commissioner, and
- Non-government privacy advocates (Australian Privacy Foundation, Liberty Victoria, Electronic Frontiers Australia)

Next steps—how you can help

We intend to hold face-to-face or teleconference consultation sessions in the week of 10 February 2014. The face-to-face sessions would be held in Canberra, Sydney and Melbourne depending on need and availability. To better inform those sessions, it would assist us to know your initial thoughts about the proposals. We have set out in the following section the questions which on which we would appreciate your thoughts. Following the consultation sessions, we anticipate that you may wish to flesh out or amend your written submissions. We are therefore proposing to ask for final written submissions, following the consultation sessions, by 28 February 2014.

Proposed consultation timetable

Initial written comments — By 7 February 2014
Consultation sessions (face-to-face or teleconference) —Week of 10 February 2014
Final written submissions — By 28 February 2014

Questions for consultation

Generally:

- Without the DVS, what other methods (paper-based, electronic, etc) can organisations use to verify the identity of individuals?
- What might be the downstream privacy impacts of those other identification processes (document copying, record keeping, etc)?

In relation to each proposal:

- What impact do the amendments to the *Privacy Act 1988* (Cth) have on the lawfulness of the proposal?
- In what circumstances could the proposal have a positive impact for individuals whose identities are being verified by an organisation?
- In what circumstances could the proposal have a negative impact for individuals whose identities are being verified by an organisation?
- In what ways can any negative impacts could be managed?
- What security or access controls should be adopted if the proposal is adopted?
- What information should individuals be given about the results from the DVS if the proposal is adopted?

Please also address any other issues you see with the proposal.

Attachment— Policy for access to the Document Verification Service by Business Users

The nationally agreed policy for the commercial DVS limits its use to businesses with legislated identification obligations. In consultation with national stakeholders, AGD is exploring the potential for expanded private sector use, initially as it might align with the recent reforms to the Commonwealth privacy regime.

Access policy context

In the first phase of extending access to DVS to the private sector, it will be provided to entities that have a client identification requirements under Commonwealth legislation. Government already regulates the operations of these agencies. Access to the DVS will take account of these existing risk-based regulatory procedures. Given all governments' stated objective is to reduce red tape for industry, DVS represents a method that can potentially streamline and reduce these regulatory burdens, rather than creating new procedures. Examples of regulatory authorities that oversee likely DVS users are:

- ACMA
- Austrac
- APRA
- Office of Transport Security
- OAIC (including the Privacy Commissioner)
- ASIC

Business Users must also be subject to the privacy regime set out under the National Privacy Principles and the Privacy Act 1988.

Principles for access

The DVS is a commercial service and will operate on commercial lines. DVS Business User Applications will be accepted on a 'first-come, first-served' basis. Private sector organisations applying to become an approved DVS Business User need to meet the following requirements:

7. are subject to the Privacy Act 1988,
8. have a demonstrable requirement under law to verify the identity of their clients
9. are employing the DVS for an appropriate use, e.g. client registrations
10. operate within a regulatory regime, e.g. a banking or financial service licencing schemes in the case of financial institutions.
11. will agree to comply with all DVS private sector requirements, e.g. obtaining the informed consent of their clients, ICT and information security controls, logging and monitoring use, compliance reporting and audits etc. , and
12. will agree to undergo independent audits of their use of the DVS

Where the DVS Advisory Board does not have a specific and material objection to the organisation and the organisation pays the applicable fees at the time of application, it will be approved as a DVS Business User.

Attachment 2 - Document Verification Service Business User Terms and Conditions of Use

Australian Government
Attorney-General's Department

Document Verification Service
BUSINESS USER APPLICATION FORM

This Application is made by:

Applicant Business (full legal entity name):			
A.C.N	A.B.N.	Other relevant registration details (if any)	
Physical Address:			Postcode:
Postal Address:			Postcode:

Applicant Business Type: (check one only)

- ☐ *cash dealer* (as defined in the *Financial Transaction Reports Act 1988* and the *Financial Transaction Reports Regulations 1990*)
  State relevant type/s of service:
- ☐ Provider of a designated service (*reporting entity* as defined in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*)
  State type/s of designated service:
- ☐ superannuation service provider (regulated parties i.e. *trustee, superannuation entity* under the *Superannuation Industry (Supervision) Act 1993,* the *Superannuation Industry (Supervision) Regulations 1994*, the *Retirement Savings Account Act 1997* and the *Retirement Savings Accounts Regulations 1997*)
  State type/s of service:
- ☐ telecommunications service provider (*carriage service providers* or *mobile virtual network operator* under the *Telecommunications Act 1997*
  State type/s of service:
- ☐ credit report provider to which applies the Credit Reporting Code of Conduct made under the Privacy Act 1988
  State type/s of service:
- ☐ Other (please describe):
  State type/s of service:

Applicant Authorised Representative:		
Name:	Position:	
Telephone:	Fax:	Email:
Nominated Gateway Service Provider *(where relevant)*:		
Name:	Position:	
Telephone:	Fax:	Email:

Applicant Privacy Policy : Please attach a copy of your privacy policy that will be applicable to your Gateway Service ☐ **CONFIRM ATTACHED**
by ticking the box

to:

Commonwealth of Australia represented by the **Attorney-General's Department**, A.B.N. **92 661 124 436** ('AGD') and each Official Record Holder.

Australian Government
Attorney-General's Department

Document Verification Service
BUSINESS USER APPLICATION FORM

1. The Applicant hereby applies to AGD to be provided with access to the Document Verification Service in accordance with the Document Verification Service Business User Terms and Conditions of Use.

2. The Applicant represents and warrants that all information provided in respect to this Application is true, correct, accurate and not misleading.

3. The Applicant acknowledges and agrees that, should AGD approve this Application, in consideration for that approval the Applicant has agreed to and will be legally bound by and must observe the Document Verification Service Terms and Conditions of Use (which the applicant acknowledges that it has received, read and understood prior to making this Application) as and from the date AGD advises the Applicant in writing that its Application has been approved.

4. The Applicant further acknowledges and agrees that in consideration of Austroads agreeing with AGD to provide Information Match Results in relation to driver license information in connection with the Document Verification Service and to perform other obligations to AGD, as and from the time the Applicant first issues an Information Match Request in respect of a drivers' licence Supported Document it will be legally bound by and must observe the Document Verification Service Terms and Conditions of Use under an additional and separate contract with Austroads.

Signed for and on behalf of the Applicant by

_____

Signature of Applicant's duly authorised representative

_____

Full name of Applicant's duly authorised representative

_____

Title of Applicant's duly authorised representative

Date / /

Australian Government

Attorney-General's Department

Document Verification Service Business User
TERMS AND CONDITIONS OF USE

Introduction

64 Your access to and use of the DVS is subject to these Document Verification Service Business User Terms and Conditions of Use (these Conditions).

Pre-conditions to DVS use

65 To be able to connect to the DVS you must:

65.1 have an operational DVS Business User ID;

65.2 either yourself be an current Approved Gateway Service Provider or have in place an arrangement with a third party current Approved Gateway Service Provider

65.3 ensure any DVS Information Match Results you receive are recorded so as to allow us to efficiently and effectively audit your compliance with these Conditions

65.4 meet all other requirements we may advise you of to enable you to access and use the DVS.

Use

66 You must ensure that all relevant members of your Personnel are aware of and comply with these Conditions.

67 You must ensure that your use of the DVS does not (and does not attempt to) modify, interfere with, disrupt, adversely affect or misuse the DVS or DVS functionality in any way, or interfere with or disrupt use of the DVS by any other person.

68 You must ensure that your use of the DVS and Information Match Data complies with all laws, regulatory requirements, and complies with all codes of conduct to which you ascribe.

69 You must promptly provide us with any information we request in respect to your access to or use of the DVS, including any routine reports and certifications.

70 You must strictly comply with all instructions and guidance we advise to you in respect to your access to and use of the DVS and Information Match Results and any other related matter.

71 Except as may be specifically authorised by us in writing, you must:

71.1 only access and use the DVS and Information Match Data to assist you in meeting your statutory obligations in relation to identity verification

71.2 not allow any person other than your authorised Personnel to access or use Information Match Data or your DVS Business User ID

71.3 only access and use the DVS and Information Match Data exclusively for your own internal purposes

71.4 not collect, store or use Information Match Results for any purpose associated with the provision, or potential provision of, an information service to any person

71.5 not use or disclose any personal information (as defined in the *Privacy Act 1988* (Cth)) obtained through your use of the DVS for any purpose other than your access and use of the DVS

71.6 not make any public statement concerning the DVS or your access to or use of it .

72 You must not, by act or omission, directly or indirectly, mislead any person in relation to the DVS, your access to or use of the DVS or any related matter.

73 You and your Approved Gateway Service Provider must fully cooperate with and support any audit or verification process we (or our agents) wish to conduct to verify your compliance with these Conditions, without limitation including providing us with prompt access to relevant records, systems, premises and facilities. You authorise us to have access to any records or information held by any Approved Gateway Service Provider relevant to your access to or use of the DVS.

Privacy, consent and information use

74 You must ensure that your use of the DVS and Information Match Data complies with the *Privacy Act 1988.*

75 You must ensure that each individual providing details in a Supported Document to you:

75.1 confirms they are authorised to provide those details to you

75.2 is informed of the purpose for which that information is sought and will be used by you (including that the information will be subject to an Information Match Request in relation to relevant Official Record Holder information, and that a corresponding Information Match Result will be provided via the use of third party systems)

75.3 provides you with their express consent for such use and accessing such information prior to any such use or access being initiated or made by you

and that you keep full and proper records of all such disclosures, confirmations and consents.

76 You must:

76.1 comply with your own privacy policy

76.2 not make any change to your privacy policy without notifying us of the change, and where possible give us no less than 30 days day prior written notice of any proposed change.

Your facilities

77 You must provide everything that you need to access and use the DVS and ensure that your equipment and facilities are properly configured and otherwise meets all relevant requirements advised by us.

Fees and charges

78 You must pay all fees and charges advised to you in respect to you being a DVS Business User. Unless specifically stated to the contrary, all fees, once incurred are payable and once paid are non-refundable, including where your access to or use of the DVS is cancelled, suspended or terminated for any reason.

Security

79 You must comply with all security procedures advised to you in relation the DVS and take all reasonable action to protect and maintain the security of the DVS and your access to and use of it, including, without limitation, maintaining the security of all tokens, access codes, encryption keys and other information relating to access, authentication or security relating to the DVS.

80 You must take all reasonable action to prevent and detect

unauthorised use of the DVS and your Business Access System.

81 You must immediately notify us if you know or suspect that access or authentication security information has been compromised or any other kind of unauthorised use or security breach has occurred, or if you know or suspect that there is a security vulnerability, fault, error or problem in the DVS or any Information Match Result.

Updates and changes to the DVS

82 The DVS may be upgraded and its features, functionality and other characteristics may change from time to time. We will endeavour to provide reasonable notice of any changes that we consider are not routine and should be advised to DVS Business Users. You acknowledge that it may not be reasonably possible to provide notice in all circumstances and that in no event will we be obliged to provide notice exceeding 14 days.

The DVS is provided 'as is' and 'as available'

83 The DVS has been implemented in a technical environment that is designed to provide high availability and be fault tolerant. However, as with any technology based facility, the speed and characteristics of the DVS will vary at different times and under different circumstances and the DVS may not always work as described, and the DVS and Information Match Results may be subject to faults, errors, interruption or breakdown or be fully or partially unavailable. You acknowledge and agree that, subject to clause 92, your access to and use of the DVS is on an 'as is, as available' basis only, and without limiting the foregoing:

83.1 you must ensure your business processes and operations can be satisfactorily conducted despite the DVS or Information Match Results being subject to faults, errors, interruption or breakdown or be fully or partially unavailable for any reason

83.2 any information we provide regarding availability, performance or other service levels or characteristics relating to the DVS, no matter how expressed, are non-contractual statements of intent only and do not constitute a representation or warranty of any kind.

84 You acknowledge and agree that you:

84.1 are solely responsible for your business processes and decisions

84.2 must, where any issues arise with your customers or other stakeholders that in any way relate to your access to or use of the DVS or Information Match Data, ensure that the relevant customers and stakeholders understand that you are the sole point of contact in relation to those issues

84.3 must manage and resolve all such issues yourself as expeditiously as possible and without seeking to involve us or in any way

Changes to these Conditions

85 We can update or otherwise vary these Conditions by not less than 45 days prior written notice to you.

Cancellation

86 We will promptly cancel your DVS Business User ID if you notify us to do so. We will advise you once cancellation has been effected.

Suspension and Termination

87 We may refuse access to the DVS, or suspend its operation in whole or in part either for you as a specific DVS Business User, for any Approved Gateway Service Provider or generally, at any time for any reason we think fit.

88 We may terminate you DVS Business User ID:

88.1 with or without cause at any time by not less than 45 days prior written notice to you

88.2 where you have breached these Conditions, immediately by written notice to you.

Indemnity

89 Subject to clause 92, you indemnify us against any loss, damage, cost, expense (including legal expenses on a solicitor and own client basis), claim, proceeding or liability of any kind that we (or our Personnel) may incur, that arises (no matter how arising including from negligence by us) out of or in connection with, your use (including unauthorised use) of your DVS Business User ID, your access to or use of the DVS, the correctness or otherwise of Information Match Results, your Gateway Service or the lawful exercise of our rights pursuant to these Conditions.

Priority

90 To the extent of any inconsistency between a provision in this document and any other provision forming part of these Conditions, the provision in this document will prevail.

Disclaimer and liability

91 You acknowledge that we provide Information Match Results based on information which may be provided to us by third parties and that where that is the case we have not independently verified the accuracy or completeness of information provided by those third parties. Subject to clause 92, the DVS and Information Match Results are made available without any representation or warranty of any kind (without limitation in respect to the accuracy of Information Match Results) and we have no liability to you in respect of any loss or damage that you might suffer no matter how arising (including from negligence by us) that is directly or indirectly related to the DVS, or Information Match Results or any other relevant matter, without limitation including any Gateway Service and, any Approved Gateway Service Provider.

92 Except as set out in this clause 92, nothing in these Conditions excludes, restricts or modifies the application of, or liability in respect of, any consumer guarantee that applies to these Conditions under the Australian Consumer Law (Consumer Guarantee). Our liability for any failure by us to comply with a Consumer Guarantee that applies to these Conditions is limited to us (at our election):

92.1 supplying the services again; or

92.2 paying the cost of having the services supplied again,

except where it is not 'fair or reasonable' (as contemplated under section 64A of the Australian Consumer Law) for us to do so.

Notice

93 We may advise or notify you of any matter in relation to the DVS and these Conditions by email, mail, facsimile or telephone to any relevant address or number that you have provided to us.

Definitions

94 In these Conditions, unless the context implies a contrary intention, the following terms have the meaning set out below:

Approved Gateway Service Provider means a provider of a Gateway Service that is at all relevant times approved by us.

Australian Consumer Law means Schedule 2 to the *Competition and Consumer Act* 2010 (Cth) and the corresponding provisions of the Australian Consumer Law (ACT) or any other state or territory as applicable.

Austroads means Austroads Ltd ACN 136 812 390.

Business Access System means systems and facilities that you use to connect to and interact with the DVS.

DVS means the system (including all associated services, infrastructure, applications, facilities, functionality, data, information and material, whether belonging to or operated by us or a third party) established by us to provide Information Match Results (but does not include any Gateway Service).

DVS Business User ID means a number or other mechanism (and associated access credentials) provided by us by which you are uniquely identified to us for purposes including accessing the DVS, transaction processing, and record keeping.

DVS Testing Environment means any system or facility we make available to you for testing purposes.

Gateway Service means the services and facilities (forming part of your Business Access System) by which your internal systems connect to the DVS.

Information Match Data means data and information in or relating to Information Match Requests or Information Match Results.

Information Match Request means an electronic request to the DVS by a User (required to be submitted in a structured electronic format advised by us) to be provided with an Information Match Result in relation to the details of relevant information in a Supported Document.

Information Match Result means, in respect to an Information Match Request, an electronic response indicating that the information provided in the request either matches or does not match the relevant official record data, or that a system error has been encountered in trying to process that request.

Official Record Holder means, in respect of each Supported Document, the entity against whose official record data the information submitted in an Information Match Request is matched (or attempted to be matched) via the DVS.

Personnel includes employees, officers, directors, contractor and agents.

Supported Document means a type of document (for example an Australian Passport or Australian Citizenship Certificate) that is supported by the Document Verification Service.

User means each person (and, if relevant, each automated system) who can initiate an Information Match Request in relation to your DVS Business User ID.

we and **us** means Commonwealth of Australia acting represented by the Attorney-General's Department and, in relation to clauses 83, 89, 91 and 92, also includes each Official Record Holder and (in the case of driver's licence information) Austroads.

you means the relevant DVS Business User, and, as the context admits, each relevant User.

Australian Government
Attorney-General's Department

Document Verification Service
Business User
Addendum 1 – Fee Schedule

Business User Application Fee

As an originator of verification requests *Business Users* will need to be approved by the DVS Advisory Board and sign a formal application. A *Business User* that seeks to use the DVS will be charged a $5,000 **application fee,** if it submits this form unamended, to cover the cost of assessing and approving applications.

Connection Fee

Businesses which establish **a direct ICT connection to the DVS** will be acting as *Gateway Service Providers* (GSPs). They may be accessing the DVS on their own behalf as an approve Business User, or in order to provide services to other *Business User* clients. GSPs will be charged $50,000 to link their systems to the DVS Hub infrastructure via Web Services, including test and 'sandpit' environments, testing processes and migration into the production environment. The connection fee includes an amount payable to current DVS IT service providers together with AGD's internal costs. The price of a non-Web Services connection will be advised on a case-by-case basis.

Transaction Fees

A tiered schedule of transaction fees is **payable by the party connecting directly to the DVS** (i.e. GSP) which will vary based on the volume of transactions. Where a GSP's annual Information Match Requests number 400,000 or less, a fee of $1.40 is proposed for each and every Request that does not encounter a DVS system error Match Result. The transaction fee progressively falls to $0.65 once the GSP's annual volume exceeds 1 million transactions per annum.

Annual Volume	per calendar month	per query charge
< 400,000	<33,000	$1.40
>400,001 <600,000	>33,000 <50,000	$1.20
>600,001 <800,000	>50,000 <65,000	$1.00
>800,001 <1 million	>65,000 <85,000	$0.80
>1 million	>85,000	$0.65

Pricing Issues

GST

GST will be levied on DVS costs.

Review

DVS prices will be reviewed annually and may decrease.

Australian Government
Attorney-General's Department

Document Verification Service Business User

Addendum 2 – Document availability by Type and Jurisdiction

Australian Driver Licences	New South Wales
	Victoria
	Queensland
	Western Australia
	South Australia
	Tasmania
	Australian Capital Territory
	Northern Territory
Medicare Cards	Australian Resident (Green)
	Interim Card (Blue)
	Reciprocal Health Care Agreement (Yellow)
Australian Travel Documents	Passport (including Ordinary, Frequent traveller, Diplomatic, Official and Emergency)
	Certificate of Identity
	Document of Identity
	UN Convention Travel Document
Australian Visas	Not including: Some Bridging Visas and Humanitarian Visas (PLO56)
Citizenship Certificates	
Registration by Descent Certificates	
Irregular Maritime Arrival Cards	Evidence of Immigration Status (EIS) ImmiCard (Pink)
	Permanent Residence Evidence (PRE) ImmiCard (Green)

Attachment 3 - Document Verification Service Gateway Service Provider Terms and Conditions of Use

Australian Government
Attorney-General's Department

Document Verification Service
GATEWAY SERVICE PROVIDER AGREEMENT FORM

This application is made by:

Applicant *(*full legal entity name):			
A.C.N	A.B.N.	Other relevant registration details (if any)	
Physical Address:			Postcode:
Postal Address:			Postcode:
Applicant Authorised Representative Name: Position:			
Telephone:	Fax:	Email:	
Applicant Privacy Policy : Please attach a copy of your privacy policy that will be applicable to your Gateway Service ☐ **CONFIRM ATTACHED** by ticking the box			

to:

Commonwealth of Australia represented by the **Attorney-General's Department**, A.B.N. **92 661 124 436** ('AGD') and each Official Record Holder.

1. The Applicant hereby applies to AGD to be approved as a Document Verification Service Gateway Service Provider.

2. The Applicant represents and warrants that all information provided in respect to this Application is true, correct, accurate and not misleading.

3. The Applicant acknowledges and agrees that, should AGD approve this Application, in consideration for that approval the Applicant has agreed to and will be legally bound by and must observe the Document Verification Service Gateway Service Provider Terms and Conditions of Use (which the applicant acknowledges that it has received, read and understood prior to making this Application) as and from the date AGD advises the Applicant in writing that its application has been approved.

4. The Applicant further acknowledges and agrees that in consideration of Austroads agreeing with AGD to provide Information Match Results in relation to driver license information in connection with the Document Verification Service and to perform other obligations to AGD, as and from the time the Applicant first issues an Information Match Request in respect of a drivers' licence Supported Document it will be legally bound by and must observe the Document Verification Service Gateway Service Provider Terms and Conditions of Use under an additional and separate contract with Austroads.

Signed for and on behalf of the Applicant by

_____

Signature of Applicant's duly authorised representative

_____

Full name of Applicant's duly authorised representative

_____

Title of Applicant's duly authorised representative

Date / /

Australian Government

Attorney-General's Department

Document Verification Service
Gateway Service Provider
TERMS AND CONDITIONS OF USE

Introduction

95 Your access to and use of the DVS is subject to these Document Verification Service Gateway Service Provider Terms and Conditions of Use (these Conditions).

Pre-conditions to DVS access

96 To be able to connect to the DVS and provide Gateway Services you must:

- 96.1 have an operational DVS Gateway Service Provider Account;
- 96.2 have a Gateway System that meets all requirements we have advised to you;
- 96.3 ensure your Gateway System has been thoroughly tested:
  - (a) within your own environment
  - (b) within the DVS Testing Environment (unless otherwise agreed in writing by us) and
  - (c) with each of your Gateway Users.
- 96.4 ensure you have complied with any Gateway System certification requirements advised by us
- 96.5 ensure your Gateway System includes a process that ensures each of your Gateway Users is properly authenticated and that the Gateway System (and other relevant systems) maintain comprehensive records of each Gateway User's use of the Gateway System and its access to and use of the DVS generally so as to allow us to efficiently and effectively audit your compliance with these Conditions
- 96.6 have obtained written confirmation from us that we have registered the relevant IP address(es) that you will use in respect to your access to and use of the DVS
- 96.7 meet all other requirements we may advise you of to enable you to access and use the DVS.

Use

97 Before accepting anyone as a Gateway User, you must ensure that they are an Authorised Business User.

98 Your contractual arrangements with Gateway Users must require you to comply with the Document Verification Service Business User Terms and Conditions of Use.

99 You must provide reasonable assistance to prospective Gateway Users to ensure they can become Authorised Business User as quickly and conveniently as possible.

100 You must ensure that all your Personnel are aware of and comply with all provisions of these Conditions that are relevant to their role, function and duties.

101 You must ensure that your Gateway System, your Gateway Services and your Gateway Users do not (and do not attempt to) modify, interfere with, disrupt, adversely affect or misuse the DVS or DVS functionality in any way, or interfere with or disrupt use of the DVS by any other person.

102 You must ensure that your (and take all reasonable steps to ensure that Gateway Users') access to and use of the DVS is properly authorised, complies with all laws, regulatory requirements, and complies with all codes of conduct to which you ascribe.

103 You must promptly provide us with any information we request in respect to your access to your Gateway System, Gateway Services and use of the DVS, including any routine reports and certifications.

104 You must strictly comply with all instructions and guidance we advise to you in respect to your Gateway System, your access to and use of the DVS and Information Match Results and any other related matter.

105 Except as may be specifically authorised by us in writing, you must:

- 105.1 not allow any person other than your authorised Gateway Users to use your Gateway Service
- 105.2 only access and use the DVS to provide your Gateway Service and for no other purpose
- 105.3 not outsource or externally host any aspect of your Gateway System or Gateway Service
- 105.4 not collect or store Information Match Results
- 105.5 not collect, store or use Information Match data for any purpose other than is strictly necessary to provide the Gateway Serviced directly to the requesting Gateway User
- 105.6 not yourself make any Information Match Requests (other than if you are also an Authorised Business User and make such requests in that capacity as Gateway User)
- 105.7 not make any public statement concerning the DVS or your access to or use of it .

106 You must not, by act or omission, directly or indirectly, mislead any person in relation to the DVS, your access to or use of the DVS, your Gateway Service, your Gateway System or any related matter.

107 You must fully cooperate with and support any audit or verification process we (or our agents) wish to conduct to verify your compliance with these Conditions, or your Gateway Users' compliance with all their obligations relating to the DVS, without limitation including providing us with prompt access to relevant records, systems, premises and facilities and ensuring you have any necessary consents from any person to do so.

Privacy, consent and information use

108 You must:

- 108.1 ensure that the data subject of each Information Match Request has provided his or her prior express consent to the provision, access and use of all personal information relevant to them that is necessary for you to provide your Gateway Service and for us to provide the DVS
- 108.2 not use or disclose any information obtained from us or your Gateway Users for any purpose other than is strictly necessary for you to provide your Gateway

Service and to comply with these Conditions

108.3 in addition to any other requirement, strictly comply with your own privacy policy relevant to your Gateway Service

108.4 not make any change to your privacy policy relevant to your Gateway Service without notifying us of the change, and where possible give us not less than 30 days day prior written notice of any proposed change.

Your facilities

109 You must provide everything that you need to provide your Gateway System and Gateway Service and to access and use the DVS and ensure that your equipment and facilities are properly configured and otherwise meets all relevant requirements advised by us.

Fees and charges

110 You must pay all fees and charges advised to you in respect to the use of your DVS Gateway Service Provider Account and your access to the DVS.

Security

111 You must comply with all security procedures advised to you in relation to the DVS and take all reasonable action to protect and maintain the security of the DVS and your access to and use of it, including, without limitation, maintaining the security of all tokens, access codes, encryption keys and other information relating to access, authentication or security relating to the DVS.

112 You must take all reasonable action to prevent and detect unauthorised use of the DVS and your Gateway System and Gateway Services.

113 You must immediately notify us if you know or suspect that access or authentication security information has been compromised or any other kind of unauthorised use or security breach has occurred in respect to the DVS, your Gateway System, Gateway Service or Gateway Users, or if you know or suspect that there is a security vulnerability, fault, error or problem in the DVS, any Information Match Result, or your Gateway System, Gateway Service or Gateway Users' systems.

Updates and changes to the DVS

114 The DVS may be upgraded and its features, functionality and other characteristics may change from time to time. We will endeavour to provide reasonable notice of any changes that we consider are not routine and should be advised to users. You acknowledge that it may not be reasonably possible to provide notice in all circumstances and that in no event will we be obliged to provide notice exceeding 14 days.

The DVS is provided 'as is' and 'as available'

115 The DVS has been implemented in a technical environment that is designed to provide high availability and be fault tolerant. However, as with any technology based facility, the speed and characteristics of the DVS will vary at different times and under different circumstances and the DVS may not always work as described, and the DVS and Information Match Results may be subject to faults, errors, interruption or breakdown or be fully or partially unavailable. You acknowledge and agree that, subject to clause 92, your access to and use of the DVS is on an ‘as is, as available’ basis only, and without limiting the foregoing:

115.1 you must ensure your business processes and operations can be satisfactorily conducted despite the DVS or Information Match Results being subject to faults, errors, interruption or breakdown or be fully or partially unavailable for any reason

115.2 any information we provide regarding availability, performance or other service levels or characteristics relating to the DVS, no matter how expressed, are non-contractual statements of intent only and do not constitute a representation or warranty of any kind.

116 You acknowledge and agree that you:

116.1 are solely responsible for your business processes and decisions

116.2 you are fully responsible for all access to and use of the DVS made via your Gateway System and Gateway Services, including use by your Gateway Users and any unauthorised use (both of which constitute your use for the purposes of these Conditions).

116.3 must, where any issues arise with your Gateway Users or other person that in any way relates to your Gateway System, Gateway Services or access to or use of the DVS, ensure that they understand that you are the sole point of contact in relation to those issues

116.4 must manage and resolve all such issues yourself as expeditiously as possible and without seeking to involve us in any way.

Changes to these Conditions

117 We can update or otherwise vary these Conditions by not less than 45 days prior written notice to you.

Cancellation

118 We will promptly cancel your DVS Gateway Service Provider Account and your access to the DVS if you notify us to do so. We will advise you once cancellation has been effected.

Suspension and Termination

119 We may refuse access to the DVS, or suspend its operation in whole or in part either for you as a specific Gateway Service Provider, or for any or all of your Gateway Users or generally, at any time for any reason we think fit.

120 We may terminate your access to the DVS or your DVS Gateway Service Provider Account:

120.1 with or without cause at any time by not less than 45 days prior written notice to you

120.2 where you have breached these Conditions, immediately by written notice to you.

Indemnity

121 Subject to clause 30, you indemnify us against any loss, damage, cost, expense (including legal expenses on a solicitor and own client basis), claim, proceeding or liability of any kind that we (or our Personnel) may incur, that arises (no matter how arising including negligence by us) out of or in connection with, your use (including unauthorised use) of your DVS Gateway Service Provider Account, your access to or use of the DVS, the correctness or otherwise of Information Match Results, your Gateway System, your Gateway Service, your Gateway Users or the lawful exercise of our rights pursuant to these Conditions.

Priority

122 To the extent of any inconsistency between a provision in this document and any other provision forming part of these Conditions, the provision in this document will prevail.

Disclaimer and liability

123 You acknowledge that we provide Information Match Results based on information which may be provided to us by third parties and that where that is the case we have not independently verified the accuracy or completeness of information provided by those third parties. Subject to clause 30, the DVS and Information Match Results are made available without any representation or warranty of any kind (without limitation in respect to the accuracy of Information Match Results) and we have no liability to you in respect of any loss or damage that you might suffer no matter how arising (including from negligence by us) that is directly or indirectly related to the DVS, or Information Match Results or any other relevant matter, without limitation including any Gateway Service and, any Approved Gateway Service Provider.

124 Except as set out in this clause 30, nothing in these Conditions excludes, restricts or modifies the application of, or liability in respect of, any consumer guarantee that applies to these Conditions under the Australian Consumer Law (Consumer Guarantee). Our liability for any failure by us to comply with a Consumer Guarantee that applies to these Conditions is limited to us (at our election):

124.1 supplying the services again; or

124.2 paying the cost of having the services supplied again,

except where it is not 'fair or reasonable' (as contemplated under section 64A of the Australian Consumer Law) for us to do so.

Notice

125 We may advise or notify you of any matter in relation to the DVS and these Conditions by email, mail, facsimile or telephone to any relevant address or number that you have provided to us.

Definitions

126 In these Conditions, unless the context implies a contrary intention, the following terms have the meaning set out below:

Australian Consumer Law means Schedule 2 to the *Competition and Consumer Act* 2010 (Cth) and the corresponding provisions of the Australian Consumer Law (ACT) or any other state or territory as applicable.

Austroads means Austroads Ltd CAN 136 812 390

Authorised Business User means a legal entity that is (at the relevant point in time) authorised by us to issue Information Match Requests to and receive Information Match results from the DVS.

Document Verification Service Business User Terms and Conditions of Use means at any point in time the then current the terms and conditions published by AGD under which access to and use of the DVS is made available to Authorised Business Users.

DVS means the system (including all associated services, infrastructure, applications, facilities, functionality, data, information and material, whether belonging to or operated by us or a third party) established by us to provide Information Match Results (but does not include any Gateway Service).

DVS Gateway Service Provider Account means an account (and associated access credentials) by which you are uniquely identified to us for purposes including accessing the DVS, transaction processing, record keeping and billing.

DVS Testing Environment means any system or facility we make available to you for testing purposes.

Gateway Service means a service that enables Authorised Business Users to connect to and interact with the DVS.

Gateway System means systems and facilities that you use to provide a Gateway Service.

Gateway User means an Authorised Business User to who you are providing a Gateway Service.

Information Match Data means data and information in or relating to Information Match Requests or Information Match Results (other than information required to be kept in accordance with clause 96.5).

Information Match Request means an electronic request to the DVS by an Authorised Business User (required to be submitted in a structured electronic format advised by us) to be provided with an Information Match Result in relation to the details of relevant information in a Supported Document.

Information Match Result means, in respect to an Information Match Request, an electronic response indicating that the information provided in the request either matches or does not match the relevant official record data, or that a system error has been encountered in trying to process that request.

Official Record Holder means, in respect of each Supported Document, the entity against whose official record data the information submitted in an Information Match Request is matched (or attempted to be matched) via the DVS.

person includes a natural person, partnership, unincorporated or incorporated association, corporation or body politic.

personal information has the meaning defined in the *Privacy Act 1988* (Cth)

Personnel includes employees, directors, officers, agents and contractors.

Supported Document means a type of document (for example an Australian Passport or Australian Citizenship Certificate) that is supported by the Document Verification Service.

we and **us** means Commonwealth of Australia acting represented by the Attorney-General's Department and, in relation to clauses 83, 89, 91 and 92 also includes each Official Record Holder and (in the case of driver's licence information) Austroads.

you means the relevant DVS Gateway Service Provider Account holder, and, as the context admits, each relevant member of your Personnel.

Australian Government
Attorney-General's Department

Document Verification Service
Gateway Service Provider
Addendum 1 – Fee Schedule

Business User Application Fee

As an originator of verification requests *Business Users* will need to be approved by the DVS Advisory Board and sign a formal application. A *Business User* that seeks to use the DVS will be charged a $5,000 **application fee,** if it submits this form unamended, to cover the cost of assessing and approving applications.

Connection Fee

Businesses which establish **a direct ICT connection to the DVS** will be acting as *Gateway Service Providers* (GSPs). They may be accessing the DVS on their behalf as an approve Business User, or in order to provide services to other *Business User* clients. GSPs will be charged $50,000 to link their systems to the DVS Hub infrastructure via Web Services, including test and 'sandpit' environments, testing processes and migration into the production environment. The connection fee includes an amount payable to current IT service providers together with AGD's internal costs. The price of a non-Web Services connection will be advised on a case-by-case basis.

Transaction Fees

A tiered schedule of transaction fees is **payable by the party connecting directly to the DVS** (i.e. GSPs) which will vary based on the volume of transactions. Where annual transaction volumes are less than 400,000 a fee of $1.40 on each and every transaction is charged. The transaction fee progressively falls to $0.65 once the annual volume exceeds 1 million transactions per annum.

Annual Volume	per calendar month	per query charge
< 400,000	<33,000	$1.40
>400,000 <600,000	>33,000 <50,000	$1.20
>600,000 <800,000	>50,000 <65,000	$1.00
>800,000 <1 million	>65,000 <85,000	$0.80
>1 million	>85,000	$0.65

Other options

Other subscription and pre-commitment options may be suggested and can be discussed with AGD.

Pricing Issues

GST

GST will be levied on DVS costs.

Review

DVS prices will be reviewed annually and may decrease.

Australian Government
Attorney-General's Department

Document Verification Service
Gateway Service Provider

Addendum 2 – Document availability by Type and Jurisdiction

Australian Driver Licences	New South Wales
	Victoria
	Queensland
	Western Australia
	South Australia
	Tasmania
	Australian Capital Territory
	Northern Territory
Medicare Cards	Australian Resident (Green)
	Interim Card (Blue)
	Reciprocal Health Care Agreement (Yellow)
Australian Travel Documents	Passport (including Ordinary, Frequent traveller, Diplomatic, Official and Emergency)
	Certificate of Identity
	Document of Identity
	UN Convention Travel Document
Australian Visas	Not including: Some Bridging Visas and Humanitarian Visas or PLO56
Citizenship Certificates	
Registration by Descent Certificates	
Irregular Maritime Arrival Cards	Evidence of Immigration Status (EIS) ImmiCard (Pink)
	Permanent Residence Evidence (PRE) ImmiCard (Green)