Australian Government
Attorney-General's Department

AGD RESPONSE TO RECOMMENDATIONS IN PRIVACY IMPACT ASSESSMENTS OF EXPANDED PRIVATE SECTOR DVS ACCESS
31 MARCH 2015

Introduction

In early 2014, the Attorney-General's Department (AGD) commissioned Clayton Utz to undertake independent privacy impact assessments (PIAs) of a proposal to expand private sector access to the Document Verification Service (DVS). Separate PIAs of the proposal were conducted:

- a Commonwealth PIA under the *Privacy Act 1988* (Privacy Act); and
- a National PIA under state and territory privacy regimes.[1]

The PIAs were undertaken to inform the decision of Commonwealth, state and territory government Ministers to expand the DVS Commercial Service at the Council of Australian Government's Law Crime and Community Safety Council (LCCSC) meeting on 4 July 2014. The expanded DVS Commercial Service commenced on 31 March 2015.

The PIAs identify some potential privacy risks associated with expanding private sector access to the DVS, but indicate that these risks are speculative in nature. The Commonwealth PIA made a number of recommendations to address the privacy impacts of expanding DVS access. The National PIA found that these recommendations would be sufficient to manage any privacy impacts under state and territory legislation.

This paper outlines AGD's response to the recommendations of the PIAs. This response is reflected in the revised DVS Commercial Service Access Policy (Access Policy) and supporting DVS Commercial Service Access Guidelines (Access Guidelines) and should be read in conjunction with those documents.

AGD agrees in-principle with the intent of all the PIAs' recommendations. In some cases, however, AGD has chosen to implement the intent of these recommendations in different ways to those recommended by the PIAs. This position is informed by the following observations.

Firstly, the obtaining of consent (both express and informed) is a contractual requirement of DVS Users in conducting DVS information matches. In many cases this is over and above DVS Users' legal requirements under the Privacy Act. The Privacy Act does not require consent for the collection of personal information where this is reasonably necessary for the organisation's functions or activities.

Secondly, we note that some of the recommendations relate to organisations' broader privacy obligations as entities subject to the Privacy Act (APP entities). The Privacy Act regulates business with a turnover of more than $3,000,000 per annum by imposing obligations as APP entities, and by empowering the Office of the

[1] *Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS* and *National Privacy Impact Assessment addressing the privacy impacts of greater private sector access to the DVS*.

Australian Information Commissioner (OAIC) as a regulator. As such, responsibility for assessing a DVS User's privacy compliance rests with the organisation itself and the OAIC, rather than AGD.

Nevertheless, AGD recognises that it is good privacy practice for organisations to implement privacy by design principles, that is, to build effective privacy controls into their policies, projects and systems. To encourage a 'privacy by design' approach, AGD has developed controls to ensure that commercial DVS Users comply with the Privacy Act, insofar as it relates to their use of the DVS, through auditing processes, contractual terms and conditions and DVS Access Policy and Access Guidelines.

Finally, expanded private sector access to the DVS brings broader benefits for the Australian community, businesses and governments, including the promotion of privacy. The PIAs themselves indicate that the DVS is less intrusive from a privacy perspective than alternative methods of identity verification as businesses no longer have a need to make copies of identity documents. Moreover, expanded access helps to combat identity crime by allowing more organisations access and use the DVS, mitigating the risks of relying on fraudulent identity documents. ID crime is recognised by all Australian governments as a major invasion of privacy.[2]

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.

Response: Agree

Compliance with the Privacy Act continues to be a contractual requirement for private sector DVS users. Users without automatic coverage under the Act are required to formally opt in through the mechanism provided by s 6EA of the Privacy Act and the Privacy Commissioner. This opt-in mechanism will obligate Users to adhere to the Privacy Act and be regulated by the Privacy Commissioner.

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.

Response: Agree

AGD respects the privacy rights of individuals and privacy considerations are at the forefront of the DVS design and operation. The current PIA process satisfies this recommendation.

The PIAs commissioned by AGD have examined the privacy impacts of expanding private sector DVS access under Commonwealth and state and territory privacy regimes respectively. These PIAs were developed in consultation with DVS and other government agencies from all jurisdictions. Two PIAs about the DVS that were previously undertaken in 2007 and 2012 have been published on AGD's website.

[2] *Intergovernmental Agreement to a National Identity Security Strategy* (2007).

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.

Response: Agree

Such reviews will be included as part of the DVS governance arrangements.

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);**
- **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).**

Response: Agree

All private sector DVS users are required to comply with the *Privacy Act 1988 (Cth)* including APP 9.2(a) (see response to Recommendation 1). The Access Policy provides that a prospective user must be able to use a government related identifier under APP 9.2 before the may apply to access the DVS Commercial Service.

The Business User terms and conditions require a prospective user to acknowledge APP 9.2 (a)-(c) and must self-assert their compliance with APP 9.2 as part of the application process for DVS access. It is a contractual requirement for Gateway Service Providers to confirm that prospective users, at all times, meet and comply with the DVS Access Criteria.

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.**

Response: Agree in-part

The new DVS Access Policy contains criteria for granting DVS access based on the language of APP 9.2 and the OAIC's *Australian Privacy Principles Guidelines.* The Access Policy is supported by the DVS Access Guidelines to help applicants understand their obligations.

AGD does not consider that the third criterion should be expressly included in the Access Policy. While this criterion appears to be related to the law enforcement exception under APP 9.2(e), it is unlikely that there will be any organisations that will apply for access to the DVS for such a purpose. This does not mean that organisations which meet APP 9.2(e) cannot access or use the DVS. All organisations which meet APP 9.2 may apply to use the DVS.

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.

Response: Agree

AGD agrees that use of the DVS should be subject to an appropriate risk-based compliance regime, that any data security or privacy breaches should be reported by the affected entity to the relevant regulatory authorities, and that all users will be subject to internal contractual remedies where appropriate. AGD is currently implementing an enhanced risk management and compliance regime, which includes targeted auditing, enhanced monitoring, and spot-checks of DVS users.

Under contractual terms for DVS access, any privacy or security breaches that *involve use of the DVS* must be reported to AGD as the DVS Hub Manager. Failure to report such an incident, or to respond appropriately to such an incident, may result in suspension or termination of DVS access. A breach of the DVS terms and conditions of use may result in legal action being taken by the relevant Gateway Service Provider (GSP) or AGD.

Privacy breaches by DVS user organisations that *do not involve use of the DVS* should be reported to the OAIC or other relevant state and territory privacy regulator. As the DVS Hub Manager, AGD will act promptly on any report of a data security or privacy breach by a DVS user organisation that it receives from the OAIC or other relevant state and territory privacy regulator. This may include considering suspension or termination of DVS access.

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

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.

Response: Agree in-principle

AGD agrees that it is important for individuals to able to lodge complaints about potential misuse of the DVS. However, AGD does not agree that it should manage the complaints process.

This recommendation replicates an existing legal requirement imposed on all APP entities, who must take reasonable steps to enable them to deal with inquiries or complaints from individuals (APP 1.2).

As APP entities, AGD, Commonwealth user agencies, Commonwealth issuing agencies, private sector users and GSPs are responsible for maintaining their own complaints processes. Responsibility for enforcing the complaints process for APP entities rests on the privacy regulator, the OAIC.

Most state and territory issuing agencies are bound by similar requirements under their respective state and territory privacy regimes and, where a privacy regime exists, are regulated by their respective privacy regulator.

Additional complaints mechanisms are also available through relevant agency or industry oversight bodies (such as Ombudsmen).

Details of these complaints processes should already be reflected in the privacy policies of DVS User organisations and GSPs, as required by APP 1.

Recommendation 8

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

Response: Agree

The National Identity Security Coordination Group (NISCG) has developed a robust audit and compliance regime which will regularly review the DVS Commercial Service taking into consideration complaints received.

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, 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]".

Response: Agree in-principle

AGD agrees that DVS users should be required to gain individuals' informed consent before any DVS checks of their personal information are undertaken. The requirement to obtain consent (informed and express) is currently included in DVS business user contracts.

The current contractual requirements for informed consent are augmented by the DVS Access Guidelines, which include suggested wording for a consent notification along the lines of that suggested by the PIA.

The Access Guidelines, not the DVS business user contract, are the appropriate place to include such details. This is because of the diversity of DVS Users' business models and their interactions with individual clients, and AGD's preference to avoid dictating Users' business processes.

Additionally, AGD requires any organisations using their own wording to submit it to AGD as the DVS Hub Manager for approval before it may be used.

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*".

Response: Agree in-principle

AGD agrees that DVS users should notify a person of the consequences of not being able to verify a person's identity to the satisfaction of the organisation. However, AGD does not agree that this should be a contractual requirement. Instead, AGD will be including the wording suggested in Recommendation 10 in the DVS Access Guidelines.

APP entities are already required to notify an individual of the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity (under APP 5.2(e)).

AGD notes that the DVS is just one tool assisting organisations to make a decision on a person's identity.

Decisions about whether and when it is necessary to verify a person's identity—and the consequences for the person of not being able to verify their identity—are matters for individual DVS User organisations (and their relevant regulatory agencies). This is separate to any decision to use the DVS.

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.

Response: Agree

AGD agrees that it is important for individuals to be able to correct information about them held by government agencies. AGD will include available contact details for DVS issuing agencies on the DVS website (www.dvs.gov.au).

AGD notes that the primary obligation for making this information available rests with APP entities under:

- APP 5.2(g), which places an obligation on APP entities to notify an individual that the privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information, and
- APP 12, which places an obligation on APP entities which hold personal information about an individual, to, on request by the individual, give the individual access to the information, unless certain exceptions apply.

These requirements extend more broadly than the operation of the DVS. Access to and correction of personal information is a matter for individual agencies and the relevant privacy regulators.