

**Report: 19 June 2023**

**Department of Transport and Planning,  
Victoria**

**OFFICIAL: Sensitive**

# PRIVACY IMPACT ASSESSMENT - JVO DIGITAL DRIVER LICENCE PROJECT



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

## Contents

Glossary	1
1. Executive summary	2
1.1 IIS's overall view	3
1.2 Recommendations	5
2. Introduction	7
2.1 PIA scope	7
2.2 About this report	8
3. Project description	9
3.1 Background	9
3.2 Project objectives and scope	9
3.2.1 Objectives and expected benefits of the project	9
3.3 Project status	10
3.4 About the DDL	11
3.5 Participants in the DDL Project MVP	12
3.5.1 The Department of Transport and Planning	12
3.5.2 JVO	13
3.5.3 34(1)(b), 34(4)	13
3.5.4 Service Victoria	13
3.5.5 Validators – Victoria Police	13
3.5.6 Validators – other	14
3.5.7 Victorian citizens using a DDL	14
3.6 Nature of systems and information flows	14
3.6.1 Key system components	14
3.6.2 Kinds of information involved	15
3.6.3 Overview of information flows	16
3.7 Legal framework	19
3.7.1 Victorian laws	19

## CONTENTS

3.8	Project governance	20
4.	Approach to risk analysis	21
4.1	Inherent privacy risks	21
4.2	Positive privacy aspects	22
4.3	Residual privacy risk level	23
5.	Findings and recommendations	24
5.1	IPP issues or risks	24
5.1.1	Transparency – IPP 1 and IPP 5	24
5.1.2	Transparency – public communications and education	28
5.1.3	Security – IPP 4	31
5.2	Governance	37
5.2.1	Project governance	37
5.2.2	Privacy by Design and future developments	38
6.	Appendix A – Methodology	40
6.1	PIA approach	40
6.2	Documents reviewed	40
6.3	Meetings held	42
7.	Appendix B – Assessment against the IPPs	43

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## Glossary

Abbreviation or term	Expansion or definition
API	Application programming interface
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
34(1)(b), 34(4)	30(1), 34(1)(b), 34(4)(a)(ii)
IIS	IIS Partners and Information Integrity Solutions Pty Ltd
IPP	Information Privacy Principles in the PDPA
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
JVO	The DTP's Joint Venture Operator for VicRoads
MVP	Minimum Viable Product
OVIC	Office of the Victorian Information Commissioner
PDPA	<i>Privacy and Data Protection Act 2014</i>
PIA	Privacy impact Assessment
QR Code	Quick Response Code
R&L	Registration & Licensing
The DTP	Department of Transport and Planning
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VicPol	Victoria Police



## 1. EXECUTIVE SUMMARY

# 1. Executive summary

The Department of Transport and Planning (the DTP), its Joint Venture Operator VicRoads (JVO) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. The DDL will be made available both through the myVicRoads and the Service Victoria platforms and apps. A DDL will allow a licence holder to access an electronic version of their licence on a mobile device and present it in place of the physical licence.

The first phase of the DDL Project is to produce a Minimum Viable Product (MVP), which would be a replication of the data and attributes from the existing Victorian driver licence to a digital credential in either the myVicRoads app or the Service Victoria digital wallet. The first release will be tested through an external pilot (early release program) with three primary use cases:

- Entitlement to drive
- Proof of identity
- The customer is over 18.

The DDL products will draw on the JVO's driver licence registry, which replicates the DTP's holding of registration and licencing (R&L) data, and which it operates on behalf of the DTP. The quantity and sensitivity of personal information involved means the privacy impacts of the DDL Project need to be carefully examined.

The DTP has engaged IIS Partners (IIS) to conduct two Privacy Impact Assessments (PIAs) on the first phase of the DDL Project. This PIA focusses on the JVO and its roles in delivering the DDL project for the external pilot and for the full DDL rollout, expected in 2024. A separate PIA will update the June 2022 PIA of Service Victoria's DDL app.

The scope of the PIA covers privacy risks associated with:

- The back-end integration to the driver licence registry, including APIs, for both products
- The design and build of the myVicRoads app
- Data flows between the JVO and the myVicRoads app
- Security of the information
- Onboarding and user experience in the myVicRoads app
- Features and use cases within the first release project scope
- Core privacy requirements under the Information Privacy Principles (IPPs).

In undertaking this PIA, IIS considered:

- Privacy principles in Victorian privacy law
- Relevant legislation such as *Road Safety Act 1986* and the *Service Victoria Act 2018*

## 1. EXECUTIVE SUMMARY

- Guidance materials published by the Office of the Victorian Information Commissioner (OVIC) and the Office of the Australian Information Commissioner (OAIC)
- Privacy good practice stemming from IIS's knowledge and experience.

This report:

- Provides background to the project, including key project participants and roles, key systems and information flows, and the relevant legal framework.
- Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

The PIA methodology is included in the Appendices.

### 1.1 IIS's overall view

IIS has not identified any high-risk privacy issues for the project with respect to implementation of appropriate controls to manage the inherent high risks. Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. The issues identified arise in the context of the project stage, which is now turning to implementation and the full-roll out, and the complexity of the project environment.

30(1), 34(1)(b), 34(4)(a)(ii)

- There is significant quantity and sensitivity of personal information involved.
- The project will involve the display of R&L data in DDLs via individuals' devices.
- The data involved includes sensitive biometrics, like driver images as well as R&L details.
- The DDL project is well advanced and has involved considerable consultation, design work, internal pilots, and independent security assessments. However, some aspects of the build and assessments are still to be completed, some documents and governance arrangements remain to be finalised and the external pilot is still to run.
- The DDL project environment is complex, with both the JVO and Service Victoria offering DDL apps, under the guidance of the DTP. The apps while developed independently are expected to meet the DTP's policy and design standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- The JVO design aims to take account of possible security risks for DDL users. However, these risks will need to be closely assessed during the pilot and will need to be monitored on an ongoing basis.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including the differences in the two apps, or how validators can interact with their devices, or handle personal information shared or displayed via the DDL – could cause concern and jeopardise uptake of the solution.

## 1. EXECUTIVE SUMMARY

While there is still work to do in some areas, many of the approaches are settled and have been tested. Taking account of the project stage – moving to the external pilot – the sensitive nature of the personal information involved, and the likely impact if it is misused (on a small or large scale), IIS considers the residual privacy risk level is medium.

Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, the development of privacy coordination and monitoring arrangements, and close attention to the possible security risks for customers using a DDL.

IIS has identified the following key privacy risks and issues for consideration at this point in the project:

- Transparency
  - Privacy policies and privacy notices – the JVO privacy policy is reasonably high-level and does not include or point to other relevant privacy information, for example, more detailed information about the DDL, the handling of personal information, and about QR codes. Collection notices also need to be finalised.
  - Public communications have been developed and should provide a good basis for public awareness about DDL and privacy and security approaches. However, in some areas the current messages lack detail or might be over-reassuring. Additional information activities are planned but not yet finalised – they will need to address a range of issues to ensure the risks as well as positives of using a DDL are known.
- Security
  - While there has been a strong focus on privacy and security by design, the potential for fraudulent or other misuse of DDLs remains – ongoing investigation and monitoring of such risks, as well as providing customers with advice will help mitigate the risks.
  - If not already, privacy risks for individuals should be included in project privacy risk registers and monitored.
- Privacy governance
  - As more detailed arrangements for ongoing project governance are settled, they need to ensure there are clear privacy roles and responsibilities, including for monitoring privacy outcomes. The governance arrangements should also ensure there is ‘no wrong door’ for privacy complaints.
  - There are a range of possible developments for the DDL that could have significant impacts on privacy. Keeping a focus on Privacy [and Security] by Design (PbD; SbD), and conducting further PIAs as needed, will be important in mitigating the possible risks.


## 1. EXECUTIVE SUMMARY




### 1.2 Recommendations

Our risk analysis takes account of the status of the DDL project and the complex environment in which it is being developed. The recommendations, which address risks identified, suggests who would be responsible for carrying out the recommendation (the DTP or JVO, or both) and the timeframe for completion. We have also noted where Service Victoria might also need to be involved.

We have specifically highlighted the recommendations that in our view must be completed before the pilot against those that should be completed within the next six months before full rollout or to be carried as an ongoing risk treatment

Legend:

IIS recommended priority to undertake risk treatment	Symbol
Before pilot	

Recommendations	Who	Timeframe
<b>Recommendation 1</b> – Project governance processes to ensure consistent, best practice privacy messages for both the myVicRoads and Service Victoria apps.	JVO & DTP and Service Victoria	For full rollout and ongoing
<b>Recommendation 2</b> – Privacy information about the DDL pilot to be prominent and easily accessible.	JVO & DTP	For full rollout and ongoing
<b>Recommendation 3</b> – Pilot collection notices to use plain English and be supported by an overview of the DDL.	JVO & DTP	For external pilot 
<b>Recommendation 4</b> – The JVO privacy policy to include comprehensive DDL information.	JVO & DTP	For full rollout and ongoing
<b>Recommendation 5</b> – Ensure DDL privacy and security information is accurate and does not overstate benefits.	JVO & DTP	For external pilot and ongoing 
<b>Recommendation 6</b> – Include privacy issues in pilot evaluation.	JVO & DTP	For external pilot 

## 1. EXECUTIVE SUMMARY

Recommendations	Who	Timeframe
<b>Recommendation 7</b> – Record DDL related privacy risks on risk register.	JVO	For full rollout and ongoing
<b>Recommendation 8</b> – Continue to assess security risks for individuals and provide up-to-date information on risks and mitigations.	JVO & DTP	For full rollout and ongoing
<b>Recommendation 9</b> – Explore options for limiting address display on the DDL driver licence view.	JVO & DTP	For full rollout and ongoing
<b>Recommendation 10</b> – Clarify requirements for the handling of individuals’ devices for DDL validation.	DTP	For full rollout and ongoing
<b>Recommendation 11</b> – Strengthen DDL privacy governance arrangements including by relevant provisions in the JVO Privacy Management Plan.	JVO	For full rollout and ongoing
<b>Recommendation 12</b> – Ensure continued PoD approach in the DDL’s further development.	JVO	For full rollout and ongoing

Released under the Freedom of Information Act 1982  
 Dept of Transport & Planning



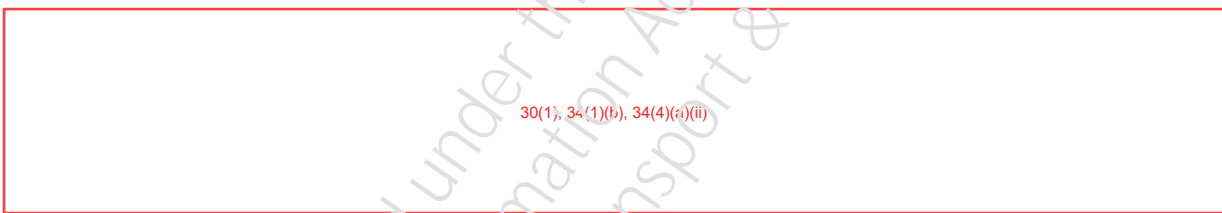
## 2. Introduction

The Department of Transport and Planning (the DTP), its Joint Venture Operator for VicRoads (JVO) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. The DDL will be made available both through the myVicRoads and the Service Victoria platforms and apps.

Both the products will leverage data from VicRoads Driver Licence registry, currently operated by the JVO on behalf of DTP. Both products have integration with DTP's driver licence registry using the new technical integration framework that the JVO is implementing as part of the DDL program. DTP provides policy oversight and guidance to ensure that the DDL products are aligned in key areas to deliver a consistent user experience to Victorian motorists.

The DTP has engaged IIS to conduct two PIAs on the first phase of the DDL Project. This PIA focusses on the JVO and its roles in delivering the DDL project. A separate PIA will update the June 2022 PIA of Service Victoria's DDL app.

### 2.1 PIA scope



This PIA covers

- JVO's delivery of the APIs, that will deliver data (1), 34(1)(b), 34(4)(a) to the JVO and Service Victoria apps
- The myVicRoads app.

It is out of scope for the PIA to assess the 34(1)(b), 34(4) JVO's activities in managing data and functions in this regard, or the processes under which individuals apply for a myVicRoads account.

The PIA will entail end-to-end consideration of privacy issues that could have an operational impact on the DDL implementation for the external DDL pilot and the expected full roll-out in 2024, from the perspective of the DTP and JVO, and for Service Victoria, to the point where the APIs connect with the Service Victoria app.

The first phase of the project is the development of a Minimum Viable Product (MVP), the first release of which will be tested in a regional external pilot (early release program) before full roll out. The purpose of this PIA is to identify any privacy issues that might arise from the project's design, build and initial implementation approaches, and to make recommendations to address any potential issues.

## 2. INTRODUCTION

In providing this report, IIS makes the following qualifications:

- The PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features.
- The PIA is based on information gathered from, and provided by, the DTP and the JVO.
- IIS does not provide legal advice; rather we provide strategic privacy and cyber security advice.

### 2.2 About this report

The report is structured to provide an overview of the DDL project, explain IIS's approach to risk analysis, analyse privacy issues according to the project scope, and provide additional context to the PIA work:

- **Project description** ([Section 3](#))  
Provides background to the DDL Project, key project participants and roles, key systems and information flows, and the relevant legal framework.
- **Approach to risk analysis** ([Section 4](#))  
Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- **Findings and recommendations** ([Section 5](#))  
Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.
- **Appendix A – Methodology** ([Section 6](#))  
Summarises our methodology, including list of documents reviewed and meetings held.
- **Appendix B – High-level assessment against the Information Privacy Principles** ([Section 7](#))  
Provides a high-level assessment of the DDL project against the Information Privacy Principles (IPPs) in the *Privacy and Data Protection Act 2014* (PDPA) and notes risks areas, which are discussed in detail in [Section 5](#).

### 3. PROJECT DESCRIPTION

## 3. Project description

### 3.1 Background

The DTP, JVO and Service Victoria are working to bring DDLs to Victorian residents. Digital licences offer customers a convenient and secure means to present a driver licence, or get their proof of age or identity details validated, where they are required to do so. Three out of six Australian state and territory jurisdictions have either trialled or have a legislation-based DDL. According to Service Victoria research, six million Victorians possess a driver licence and 80% of the licence holders would value a digital driver's licence.

The DDL will replicate data and attributes from an existing plastic Victorian driver licence to a digital credential. Initially there will be three primary use cases:

- Entitlement to drive whilst on the road
- Casual proof of that user is over 18 and photo for licensed venues and businesses such as supermarkets, convenient stores, tobacco retailers, etc.
- Proof of identity – It will be up to the third-party organisation to decide whether or not to accept the DDL for these use cases.<sup>1</sup>

The DDL products will support verification and, for Service Victoria sharing of the information, presented on various DDL views using QR code scanning (using the myVicRoads or Service Victoria apps). This feature will enable individual and business customers to validate the details presented by a DDL holder without requiring specialised hardware or facial recognition.

The project is currently working towards a first release, commencing with an external pilot (early release program). At this stage, the DDL will be supplementary to the physical driver licence and will not replace it. While most full licence drivers do not need to carry a physical licence, where the existing laws do require this, they remain enforceable. For example, the introduction of DDLs does not change the obligation of motorists such as learner and probationary drivers to carry their physical licence with them at all times.

### 3.2 Project objectives and scope

#### 3.2.1 Objectives and expected benefits of the project

The DDL is consistent with the Victorian Government's digital strategy, which is expected to deliver cost savings, and better, fairer, and more accessible services, and a digital ready economy.

---

<sup>1</sup> There will be ID verification circumstances where a DDL will not be sufficient and a DDL might be needed. For example, the first release will not provide for validator to take a copy of DDL ID details.

### 3. PROJECT DESCRIPTION

The expected benefits of the DDL for Victorian drivers are:

- Freedom – As noted, unless required to by law, most customers will be able to leave their physical licence and wallet at home (although they might still need a plastic licence, for example, to prove identity in some circumstances).
- Peace of mind – Customers know their DDL is always on their phone as a backup.
- Convenience – 89% of the customer Service Victoria consulted indicated that they believe the DDL to be more convenient than a physical driver licence because they always carry their phone with them.
- Security – No personal information is stored on the customer's device, and setup of the myVicRoads app includes multi-factor authentication (MFA) and future use requires a user login, and a six-digit PIN or biometric.
- Privacy – Customers will have a choice of how to display the DDL on their device depending on the use case (entitlement to drive, proof of age, proof of ID). If a validator seeks to confirm details displayed on the device via the QR, no personal information, other than licence number on the licence view, is shared. The QR code only confirms the details are correct or provides various limited error codes if for some reason the information cannot be verified.
- Up-to-date data management – Customers using a DDL have access to up-to-date information about the status of their licence; for example whether it is valid or has expired.

### 3.3 Project status

The DTP, JVO and Service Victoria are taking an iterative approach to the DDL project. There has been considerable ongoing consultation and collaborative development work, which for Service Victoria included an internal pilot.<sup>2</sup>

The project is now in the 'realise' stage and is moving towards an external pilot. For the JVO:

- 30(1), 34(1)(b), 34(4)(a)(ii)
- 30(1), 34(1)(b), 34(4)(a)(ii)
- The app development and build are close to finalised. There is some design work still to complete to take account of the DTP design standards.
- There is some further work on implementing the communications and engagement plan, developing governance structures, and developing privacy statements and other privacy communications.

<sup>2</sup> The internal pilot tested the Service Victoria's DDL's end-to-end journey, including identity verification, adding the DDL to the Service Victoria's Digital Wallet and the communication between Service Victoria and the DTP systems.

### 3. PROJECT DESCRIPTION

The external pilot will start in Ballarat in July 2023, with other locations following by the end of October. The myVicRoads and Service Victoria websites are currently inviting people to register for the pilot.<sup>3</sup> Sequential early release in regional locations will allow for feedback, iteration and targets to be achieved as volumes increase. Starting in July with 250 customers, the program will progressively ramp up until the 5,000 target is achieved (2,500 Service Victoria app and 2,500 myVicRoads app). Subject to outcomes of the initial pilot period, probationary and learner licence might be added to the pilot later in 2023.

Again, subject to the outcomes of the pilot, there will be a full rollout of DDL in 2024. The DDL steering committee will decide on the acceptance and rollout of the DDL products.

#### 3.4 About the DDL

The DDL is the first product in the VicRoads app and will be available through the MyVicRoads portal. DDL Customers will be able easily show an identical digital version of their driver licence, and to have certain details verified, via their myVicRoads app. Initially, the DDL could be used in three cases:

- Entitlement to drive
- Proof of identity
- Verification that the customer is over 18.

The DDL acts in a similar fashion to a physical licence however some details can be hidden by default to respect the user's privacy. The DDL effectively contains three cards. The myVicRoads app landing screen provides customers with the opportunity to select the digital card that best suits the context. The customer has the ability to show and verify subsets of their DDL details. For example, a validator scanning an age card, only sees the fact they're over 18, rather than their exact birthdate, driver licence number, address and other information, which is all apparent on a physical licence. Similarly, a scan of the identity view only indicates 'identity verified' rather than sharing any details from the licence.

The DDL will contain features, such as holograms, manual refresh, display of the last refreshed date and time and a watermark, that are digitally equivalent to the features that indicate a plastic licence is legitimate. The DDL will also include a QR code that validators (organisations seeking to rely on a DDL) can scan to verify the licence is valid. The scan displays a green tick for valid cards or an error message (for example, QR code expired, invalid QR code). The DDL also contains a bar code, which contains only the customer's licence number, and for Victoria Police (VicPol) use.

---

<sup>3</sup> See <https://www.vicroads.vic.gov.au/licences/digital-driver-licence> and <https://service.vic.gov.au/early-access/digital-driver-licence/home>



### 3. PROJECT DESCRIPTION

The JVO is taking a cautious approach to privacy and security in this first iteration of the DDL. 30(1), 34(1)(b), 34(4)(a)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii) This means that personal information will be displayed on a customer's device when they activate the app but no personal information will be stored on the device. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

While there are differences in approach, IIS considers that both the JVO and Service Victoria products have been designed and implemented with emphasis on data security and privacy (privacy and security by design). The DTP will also ensure the digital driver licence experience, design, functionality and features will be same across both DDL channels.

At this point, the products are not interoperable 30(1), 34(1)(b), 34(4)(a)(ii). This means that the JVO QR code can only be scanned with the JVO app and visa versa. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

To set up a myVicRoads DDL, customers must first have a myVicRoads account 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

DDLs are protected by the user's phone password (if used) and are only accessible by logging into the JVO app via a user login, biometric identification, or six-digit PIN, and an additional authentication step (multi-factor authentication (MFA)).

### 3.5 Participants in the DDL Project MVP

This section sets out the participants in the DDL project at the external pilot and full roll out phases.

#### 3.5.1 The Department of Transport and Planning

The DTP operates and coordinates Victoria's transport network, the delivery and upgrade of transport infrastructure, as well as the reforms to road safety policy, regulatory and legislative environment. The DTP will remain the owner of the R&L data.

The DTP is also the policy owner of driver licensing policy. All the elements that relate to licence information, entitlement to drive, safety and roads will stay with the DTP. The user's licence features and potential changes (e.g., addition of a licence, expiration, suspension) are managed on the DTP's side, and the JVO and Service Victoria only reflect those changes through the DDL.

The DTP provides policy oversight and guidance to ensure that the DDL products are aligned in key areas to deliver a consistent user experience to Victorian motorists.

### 3. PROJECT DESCRIPTION

#### 3.5.2 JVO

The JVO is providing registration and licensing services under a Concession Deed (the Deed) on behalf of the DTP. In summary it is responsible for customer service and operational activities 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii) initial customer complaints, and management of the IT systems.

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii) The APIs will allow near-real time driver licence data to be retrieved by the front-end mobile apps developed by the JVO and Service Victoria.

The JVO is also responsible for the DDL app solution design and build and will host the DDL in the myVicRoads app on the myVicRoads portal. It is responsible for the maintenance of the app and, subject to the Deed and the DTP policy and design standards, for ensuring that the right security, privacy and compliance features are in place. The JVO is also responsible for the communications with customers and will provide a digital channel for customer feedback about the DDL and pass complaints in relation to the DDL to the DTP.

#### 3.5.3 1), 34(1)(b), 34(4)(a)

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.5.4 Service Victoria

Service Victoria will, as noted, be a supplier of a DDL app. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.5.5 Validators – Victoria Police

VicPol is a key stakeholder for the DDL and is working with DTP to identify and resolve any issues.

The external regional pilot will be used to test the efficacy of, and seek feedback on, the VicPol app already available to check the barcode, which IIS understands contains only the licence number. VicPol will only be checking the DDL as an initial check. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii) The pilot will help identify any needed modifications of police processes if/when the DDL is a legally binding driver licence, 34(1)(b), 34(4)

30(1), 34(1)(b), 34(4)(a)(ii)

### 3. PROJECT DESCRIPTION

#### 3.5.6 Validators – other

For the external pilot, a number of businesses that need to validate licences or identification will be selected in Ballarat, these will include:

- National Retailers Licensed venues such as bars, pubs, nightclubs and restaurants
- Hotels
- Petrol service stations
- Supermarkets and grocery stores
- Convenience stores
- Tobacco retailers
- Licensed premises, parcel pickup and delivery businesses, retailers offering click and collect, credit options and equipment hire.

IIS notes that the initial focus will be on small businesses that do not need to retain documentary evidence of identity. Such requirements might be considered in further iterations of the DDL.

#### 3.5.7 Victorian citizens using a DDL

The external pilot will take place in the regional centre of Ballarat, only for drivers with a full licence including car, motorcycle, light, heavy vehicles. DTP estimates that the early adopters of the DDL will represent around 25% of the Ballarat population with a full licence, which means approximately 25,056 users for the external pilot.

The DTP expects the DDL will be extended to all licence holders including probationary drivers and learner drivers in further stages of the project.

### 3.6 Nature of systems and information flows

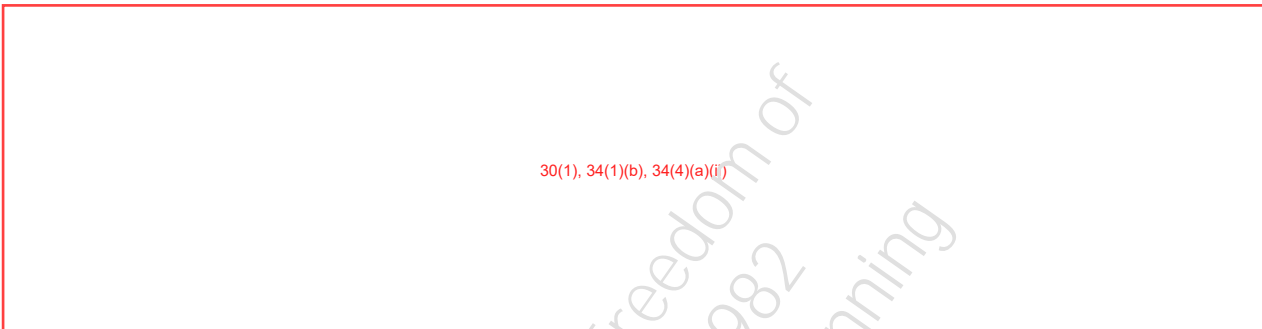
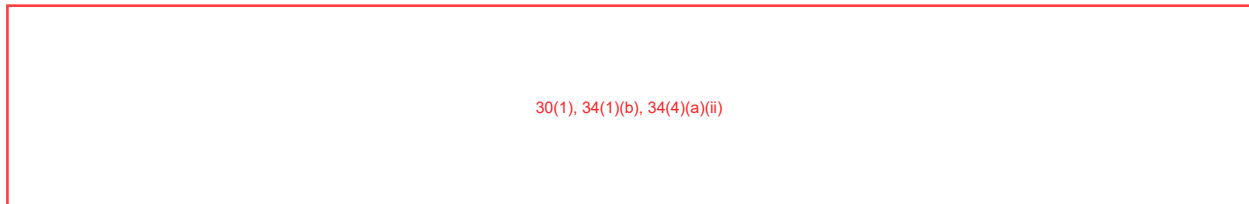
#### 3.6.1 Key system components

##### 3.6.1.1 The DTP

30(1), 34(1)(b), 34(4)(a)(ii)

### 3. PROJECT DESCRIPTION

#### 3.6.1.2 JVO



#### 3.6.1.3 Licence holders

Licence holders will use their own devices to set up, or use, a myVicRoads account, and to add a DDL to the myVicRoads app.

### 3.6.2 Kinds of information involved

#### 3.6.2.1 Personal information

The kinds of personal information JVO will display on the DDL is the same as that which currently appears on the plastic licence. As outlined, not all the information will be displaced for all views. The full set of personal information is:

- Full name
- Date of birth
- Address
- Signature
- Photo
- License number
- License expiry date
- Licence type (car/bike/dual)
- Licence proficiency (full/probationary)
- Licence category (heavy vehicle categories)
- Licence conditions

### 3. PROJECT DESCRIPTION

- Card Number (if allocated)
- Issue Date
- Licence Status.

#### 3.6.2.2 Sensitive information and health information

Depending on the licence view, the JVO DDL could also display some limited medical information about licence holders. This is in the form of conditions included on driver licences (e.g., use of glasses when driving). While the conditions are not described, the meaning of the codes is readily available. IIS considers the codes that are associated with a medical condition meet the definition of health information.

The JVO DDL will also display biometric information in the form of the licence photo and signature. Biometric information is not currently explicitly contained in the definition of sensitive information in the *Privacy and Data Protection Act 2014*. However, it is considered sensitive information under the *Privacy Act 1988* (Cth) and OVIC advises organisations to consider treating biometric information as 'delicate information' and to handle it cautiously.<sup>4 5</sup>

#### 3.6.3 Overview of information flows

At a high level, the arrangements for the JVO DDL are expected to involve the following:

- The DTP will share its R&L data with JVO under the Deed 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)
- 30(1), 34(1)(b), 34(4)(a)(ii)  
), 34(1)(b), 34(4)(
- New customers will be able to sign-up for a myVicRoads account and login using the in-app workflows provided by the mobile app. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)
- 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) The purpose of QR code to verify licence details are accurate as per the registry. When the app 'activated', DDL information and images are retrieved using QR code 30(1), 34(1)(b), 34(4)(a)(ii) and displayed on device.
- Customers can choose to show their DDLs to validators (law enforcement agencies, or businesses seeking proof of identity or age).
- Validators can also scan the QR code which will return a green tick or an error message.
- VicPol can scan the barcode, which contains the licence number, and this comes up with licence number.

The following diagram provides an overview of the DDL architecture.

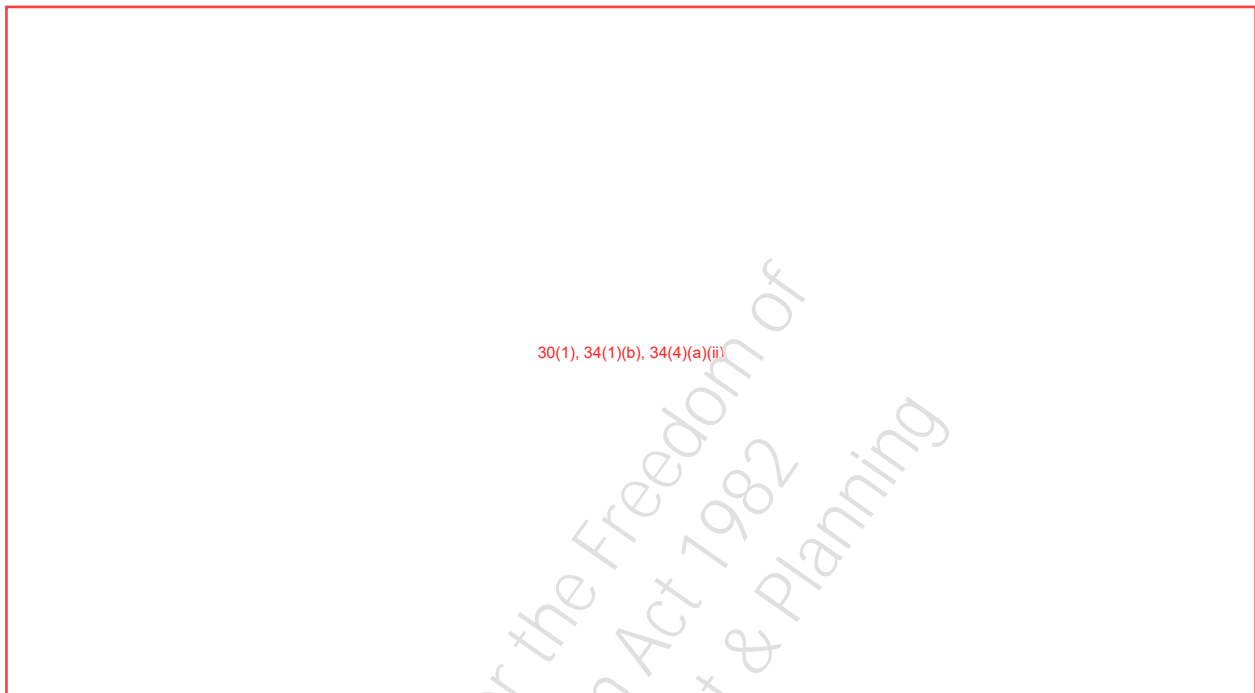
<sup>4</sup> Please refer to the definition given by OVIC: "‘Delicate information’ refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regard as requiring a higher degree of protection.", available at [https://ovic.vic.gov.au/book/key-concepts/#Sensitive\\_and\\_delicate\\_information](https://ovic.vic.gov.au/book/key-concepts/#Sensitive_and_delicate_information)

<sup>5</sup> See <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>



### 3. PROJECT DESCRIPTION

Diagram 1 – Solution overview – JVO DDL



The table below sets out the expected information flows for the creation of a DDL in the myVicRoads app. It also describes the information flows when a QR Code is generated and validated using the myVicRoads app (both by the customer and the validator).

Steps for the user	Back-end processes
Log into the app / create an account	
<p>The customer must first have, or set up, a myVicRoads, <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <p><span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <p><span style="border: 1px solid red; padding: 2px;">34(1)(b), 34(</span></p> <p>The path to the DDL is via the myVicRoads portal – it is relying on established identities.</p> <p>When they have a myVicRoads account the customer would download the myVicRoads app and login.</p>	<p>The process of setting up a myVicRoads account is outside the scope of the PIA.</p> <p>If an account is created, email address and mobile phone (if provided) are verified via the use of a one-time password. <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <div style="border: 1px solid red; height: 150px; width: 100%; margin-top: 10px;"> <p style="text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>

### 3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
Linking customer record to licence	
<p>To access a DDL for the first time, the customer will have to enter key attributes (licence no. surname, other names, address, card serial no. if affected by data breach, date of birth) into the app.</p>	<div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
Adding the DDL to the wallet	
<p>The customer can now access the DDL from the JVO app.</p>	
QR Code generation and validation	
<p><b>Generating a QR Code:</b></p> <p>The user will be given the choice to decide on different sharing options. This will allow them to determine how much of their driver licence information they'd like to show to non-law enforcement validators.</p>	<p>As noted, the JVO is not storing any personal information on mobile device. <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
<p><b>Validating a QR Code:</b></p> <p>Businesses that require proof of age, proof of ID, or proof of eligibility to drive will be able to scan the QR code to verify its validity and the validity of the details in question.</p>	<div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>

### 3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
<p>Law enforcement agencies checking licences will focus on licence number. The DDL will contain a barcode that contains the licence number</p>	<div style="border: 1px solid red; padding: 20px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>

## 3.7 Legal framework

### 3.7.1 Victorian laws

The DDL project must comply with the following relevant laws.

#### 3.7.1.1 Privacy and Data Protection Act 2014

The *Privacy and Data Protection Act 2014* (PDPA) regulates the handling and protection of personal information by Victorian public sector organisations. Organisations subject to the PDPA must comply with the IPPs that contain requirements across the information lifecycle. Part 4 of the PDPA gives the Victorian Information Commissioner the power to prescribe security requirements pertaining to public sector information and information systems through the Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS).

Section 84(3) of the PDPA provides for organisations to be declared subject to the PDPA. Gazette S523 4/10/22 declares the JVO to be a body to which Part 4 of the PDPA applies.

#### 3.7.1.2 Health Records Act 2001

The *Health Records Act 2001* (HRA) and its Health Privacy Principles (HPPs) regulate the collection, handling and protection of health information, which includes information or opinion about the physical or mental health or disability of an individual.<sup>6</sup>

#### 3.7.1.3 Road Safety Act 1986

The *Road Safety Act 1986* (RSA) is the main piece of legislation that regulates the use of roads, registration of vehicles and driver licensing in Victoria.

<sup>6</sup> The HPPs are substantially similar to the IPPs. For the purposes of our privacy analysis in Section 5, IIS has focused on the IPPs.

### 3. PROJECT DESCRIPTION

Part 7B contains the protective framework for R&L information, including the allowed purposes for use and disclosure of relevant information, the exceptional circumstances for the use and disclosure of relevant information, the uses of relevant information for verification purposes, etc

#### 3.7.1.4 Charter of Human Rights and Responsibilities Act 2006

The *Charter of Human Rights and Responsibilities Act 2006* (the Charter) is a Victorian law that sets out the protected rights of all people in Victoria as well as the corresponding obligations on the Victorian Government. The DTP will be conducting a Charter assessment with particular focus on engagement or limitation of the right to privacy.

#### 3.7.1.5 Road Safety (Drivers) Regulations 2019

Regulation 63 of the Road Safety (Drivers) Regulations 2019 describes the details that driver licence or learner permit documents must contain, including the identification number, the person's first name, second and third initials (if any) and family name; a photograph of the person; the person's residential address; the person's date of birth; a reproduction of the person's signature; the category or categories of driver licence; its expiry date; and the code of any condition to which the licence or permit is subject.

### 3.8 Project governance

The project governance arrangements take account of the fact that the JVO is providing services to the DTP under a Concession Deed (the Deed), and the DDL project is authorised by Cabinet. The Deed sets out the JVO's and DTP's role and obligations, including for privacy and security. The DTP is effectively the regulator of the JVO under the Deed. The formal governance arrangements include:

- Ministerial oversight via monthly ministerial meetings
- Steering committee with senior staff from the DTP and Service Victoria
- Working groups sitting under the steering committee with weekly meetings; the JVO participates in relevant working groups (but not the steering committee).

## 4. APPROACH TO RISK ANALYSIS

### 4. Approach to risk analysis

In undertaking this PIA, IIS considered:

- The IPPs in the PDPA
- Guidance materials published by the OVIC and the OAIC
- Privacy good practice stemming from IIS's knowledge and experience.

The PIA focuses on privacy risks that are introduced or heightened by the DDL Project, rather than privacy risks for existing processes to issue and use driver licences.

This section assesses the project's residual privacy risk level, by weighing the inherent privacy risks against the existing privacy positive aspects.

The following section discusses the project's privacy issues and risks identified in detail and makes recommendations to mitigate the risks.

#### 4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks. Inherent privacy risks arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential (including value) for, and consequences of, misuse
- The range of people from whom the information may be collected
- The context in which personal information is handled – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the project
- The extent to which information is accessed or handled by third parties
- The likely community and/or media interest in the privacy aspects of the project.

30(1), 34(1)(b), 34(4)(a)(ii)

- The quantity and sensitivity of personal information involved, as noted for example, in the DTP's Information Value Assessment.
- The project will involve the display of R&L data in DDLs via individuals' devices.
- The data involved includes driver images as well as R&L details.
- The DDL project is well advanced and has involved considerable consultation, design work, internal pilots, and independent security assessments. However, some aspects of the build and assessments are still to be completed, some documents and governance arrangements remain to be finalised and the external pilot is still to run.



## 4. APPROACH TO RISK ANALYSIS

- The DDL project environment is complex, with both the JVO and Service Victoria offering DDL apps, under the guidance of the DTP. The apps while developed independently are expected to meet the DTP's policy and design standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- The JVO design aims to take account of possible security risks for DDL users. However, there is still potential for risks to be greater than expected or for unforeseen risks to arise and so for a need for risks to be closely assessed during the pilot and monitored on an ongoing basis.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including the differences in the two apps, or how validators can interact with their devices, or handle personal information shared or displayed via the DDL – could cause concern and jeopardise uptake of the solution.

### 4.2 Positive privacy aspects

IIS considers that the DDL Project has important positive aspects that support privacy and minimise the inherent risks associated with the project. These are outlined below:

#### Positive privacy aspects with the project/solution design

- The JVO has followed the key privacy enhancing strategy of data minimisation – there will be minimal personal information transferred to display on the customer's device and data is retrieved afresh and displayed each time a customer uses the device; no personal information is stored on the device. There is no persistence of data in the networks, and data is encrypted at all stages, from the APIs, through the 'pipes' onto the app.
- The DDL project design appears to avoid the risk of a new digital footprint, in that neither the JVO or the DTP will have any detailed records that would enable them to track when, or to whom, a customer presents their DDL for checking. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)
- The DDL does not rely on the creation of duplicate stores of personal information. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) This means the DTP data remains the single 'source of truth' for driver licence information.
- The device does not hold any personal information. Each time a customer uses or refreshes the DDL, the relevant information is retrieved from the server. When a QR Code is scanned, it requests a verification of the licence and its data from the VicRoads servers, and a response is returned, which confirms but does not provide the details on the licence. The QR code is generated by a call to the DTP, and, following validation, is only available for display without refresh for two minutes.
- JVO and DTP express a strong commitment to privacy and privacy appears to have been in mind for the project design and for the implementation, although some steps remain implement appropriate governance arrangements and to support privacy requirements.

## 4. APPROACH TO RISK ANALYSIS

- The arrangement between DTP and JVO are governed by privacy legislation and by the Deed, which includes the roles and responsibilities of both parties as far as privacy and security obligations.

### Privacy advantages for DDL users over the existing plastic driver licence

- The DDL is potentially more secure in that it is protected by device and JVO app security measures, including MFA as the app is set up on a device and password or PIN or biometric protection for each use.
- The DDL includes a range of other security features.
- If an individual's device is lost or stolen, this does not mean the information is lost. A user can, with relative ease, add their DDL to another device.
- A customer's DDL can be validated in real-time. This means data can be instantly verified using by scanning the QR code displayed on the DDL within the JVO app.
- DDL users will have some choice about what information they display to validators – the app will have three 'cards', which will display only relevant details, for example, the identity card will display the customer's photo, date of birth, and address, but not their driver licence details.

### 4.3 Residual privacy risk level

Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. Rather, the issues identified arise in the context of the project stage, which is now turning to implementation and the full-roll out, and the complexity of the project environment.

While there is still work to do in some areas, many of the approaches are settled and have been tested. Taking account of the project stage – moving to the external pilot – the nature of the personal information involved, and the likely impact if it is misused (on a small or large scale), IIS considers the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, the development of privacy coordination and monitoring arrangements, and close attention to the possible security risks for customers using a DDL.

## 5. FINDINGS AND RECOMMENDATIONS

# 5. Findings and recommendations

This section discusses relevant privacy risks and issues that IIS has identified during the PIA.

The recommendations focus on mitigating privacy risks and improving practice during the final development stages, including the external pilot and full rollout of the myVicRoads DDL. 30(1)(b), 34(4)(a)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

## 5.1 IPP issues or risks

A high-level analysis of phase 1 of the DDL project against the IPPs is at [Appendix B](#). IIS considers that the DDL project would be mostly consistent with the IPPs. In particular:

- The project operates within the existing DTP's legal framework.
- The Deed authorises the JVO to collect, use and disclose personal information consistent with its roles in providing DDL infrastructure and the myVicRoads app.
- Anonymity is not practicable.
- The project will operate within Victorian borders.

The main IPPs where IIS has identified issues are in relation to openness, security, and access and correction, and privacy complaint handling.

### 5.1.1 Transparency – IPP 1 and IPP 5

Transparency provisions in the IPPs aim to allow individuals to make informed choices about providing information or using a service and to have a general understanding of how information about them is being handled. Transparency is both a matter of compliance as well as key to building public confidence and trust in the DDL.

The IPPs provide two transparency mechanisms:

- Specified details, usually a collection notice, provided at the point personal information is collected or as soon as possible thereafter (IPP 1.3)
- General information, usually via a privacy policy, about the type of personal information agencies collect and hold and how it is managed (IPP 5.1).

The Deed, at clause 39.6, mirrors these requirements and adds specific requirement to specify any law that requires collection of personal information by the State, or that personal information may be disclosed to the State. Clause 39.7 provides that collection notices must be provided to, or approved by, the Secretary [of DTP].

## 5. FINDINGS AND RECOMMENDATIONS

In keeping with its policy and oversight roles for the DDL and the 'one licence, two channels' approach, the DTP will be seeking to ensure consistency in collection notices for the myVicRoads and Service Victoria apps. IIS was advised that the JVO has not yet finalised its collection statements. IIS understands that the JVO and Service Victoria will collaborate as the notices are finalised.

The IIS assessment drew on information provided, including terms and conditions (T&C) for myLearners, and what we have seen of the JVO's approaches in other contexts (for example, viewing the VicRoads website). IIS has noted the following factors that we understand are relevant to the development of collection notices:

- Customers will need to have a myVicRoads account and a full licence to participate in the pilot; the pilot will involve limited or no additional collection of personal information.
- To use the myVicRoads app, customers have to have, or set up, a myVicRoads account. The account is the point at which JVO is collecting personal information, there is no additional collection of personal information for the pilot, other than to indicate interest, or to set up or use the myVicRoads app.
- The JVO's disclosure of personal information for DDLs, other than displaying driver licence information to the customer, is very limited. The only personal information it will disclose will be when a validator scans the QR code or bar code for the driver licence view; in this case if the licence is valid, 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) Customers may also choose to allow a validator to see, and take notes of, the information on their device.

We understand JVO's general approach to providing privacy information, including collection notices, for the pilot and the full DDL rollout will be as follows:

- Provide link to the Privacy policy on the VicRoads website<sup>7</sup>
- For myVicRoads account, provide a link to the T&C, which include a privacy statement – effectively a collection notice – and a link to the VicRoads privacy brochure
- Registering for the pilot:
  - Provide general advice, including FAQs, about the privacy and security features of the DDL, for example: 'with digital ID, you control what information you share, and who you share it with', 'having a digital driver licence in our myVicRoads app means your identity is kept safe using state-of-the-art security and privacy features', and the DDL is an 'easy, secure and private way' to access a licence, 'privacy and security of personal information is the highest priority in the digital driver licence's development'.<sup>8</sup>
  - Provide link to T&C at the point a customer logs into myVicRoads account to register for the pilot
- When setting up the app, providing a link to T&C and the privacy brochure

<sup>7</sup> <https://www.vicroads.vic.gov.au/website-terms/privacy> viewed 11 June 2023

<sup>8</sup> <https://www.vicroads.vic.gov.au/licences/digital-driver-licence> viewed 11 June 2023

## 5. FINDINGS AND RECOMMENDATIONS

- Within the myVicRoads app, the Settings menu includes 'help and info' section, with links to T&C and privacy policy
- Within the app, message on screen alerting customers to what QR code will show and validate if scanned, for example 'the person who scans this code will only validate your licence number [or 'your age/identity', or 'your age']. No other data will be shared'.<sup>9</sup>

IIS considers that this approach is likely to be consistent with the IPPs. It provides the necessary information and adopts a 'layered' approach, particularly with the short privacy messages below the QR code. However, if the JVO approach in other context is used for the DDL, the language is fairly formal and there is no easily available comprehensive plain English detail on the DDL process and handling of information.

We have identified some areas where additional action would contribute to good privacy practice.

- 30(1), 34(1)(b), 34(4)(a)(ii)
- Privacy information is not prominent on the JVO website – a search is needed to find the privacy policy
- The JVO privacy policy we viewed provides fairly general information only about the JVO's handling of personal information. We consider it would be good practice to include specific information about the JVO's role in managing R&L data, and about the DDL, in the policy, or provide links to comprehensive information elsewhere.  
This might include:
  - Collection and handling of information for identity verification
  - Data security, including steps to take if a device is lost or stolen
  - QR Codes, including what they contain and how refreshed
  - Licence or credential validator handling a device
  - How to report a device as lost or stolen to the JVO and/or to VicPol.
- The current information about the DDL pilot provides high-level assurances about privacy and security and some additional information, but it is not clear that the JVO will be providing comprehensive, detailed information about the operation of DDL's including the handling of personal information, security issues and protecting against risks, how the QR code works and so on.
- While privacy information will be available once a customer enters the myVicRoads portal, there appear to be no privacy links or information (other than, as noted, high-level assurances) from the initial pages about the pilot (or the myVicRoads account).

<sup>9</sup> MyVicRoads Digital Driver Licence Feature: QR Code, images on page 5

## 5. FINDINGS AND RECOMMENDATIONS

In the first PIA IIS undertook of Service Victoria's DDL approach, we reviewed a draft collection notice for the pilot. IIS supported the clarity of the notice and did not find any issues under IPP 1.3. The draft notice used plain English and gave a reasonably detailed overview of the Service Victoria DDL. IIS understands the JVO is aware of this notice and will take it into account in further work collection notices.

We make the following recommendations to address the issues identified.

### Recommendation 1 – Project governance processes to ensure consistent, best practice privacy messages for both the myVicRoads and Service Victoria apps

Establish project governance arrangements that include processes to ensure that privacy messages delivered by the DTP, the JVO and Service Victoria are consistent, comprehensive and adopt best practices approaches. Make clear in the governance processes who is responsible for signing-off on privacy materials and monitoring their use.

**Who:** The DTP, the JVO and Service Victoria

**Timeframe:** For full rollout and ongoing

### Recommendation 2 – Privacy information about the DDL pilot should be prominent and easily accessible.

Include comprehensive, plain English information about the operation of the DDL made available from the public web pages about the pilot. This should include information about the handling of personal information, security issues and protecting against risks, how the QR code works and so on.

**Who:** The JVO and the DTP

**Timeframe:** For the external pilot

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 3 – Pilot collection notices to use plain English and be supported by an overview of the DDL.

In developing privacy collection notices for the pilot, adopt a 'good practice' approach, consistent with Service Victoria' notice, which should include using engaging plain English and provide, in addition to the requirements of IPP 1.3, an overview of the JVO's DDL, including the information handling, the server retrieval process and the QR Code.

**Who:** The JVO and the DTP

**Timeframe:** For the external pilot

### Recommendation 4 – JVO's privacy policy to include or link to comprehensive DDL information.

Include comprehensive DDL information for the full public rollout in the JVO's privacy policy, or in links from the privacy policy.

Include an additional 'extra privacy information' section in the policy or in relevant links on the information handling for DDLs, which should cover matters such as:

- Collection and handling of information for identity verification
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential validator handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

**Who:** The JVO and the DTP

**Timeframe:** For full rollout and ongoing

### 5.1.2 Transparency – public communications and education

In addition to the specific requirements in the IPPs, active public awareness and education for DDL users and validators will support transparency about the project, and support individuals' ability to exercise their privacy rights and to use a DDL safely.

IIS is encouraged by the work DTP, JVO and Service Victoria have done to date in this area. In keeping with its role in ensuring the DDL experience, design, functionality and features will be same across both channels, DTP is taking the lead on DDL communications and engagement.



## 5. FINDINGS AND RECOMMENDATIONS

The DTP, in collaboration with the JVO and Service Victoria, has developed a Communications and Engagement Plan (the C&E Plan).<sup>10</sup> The C&E includes the narratives and key messages for the regional pilot as well as communications and engagements tactics and timings in preparation for the full rollout. The narratives and key messages provide a good high-level overview of the solutions offered by both Service Victoria and the JVO.

The Communications Team is also working on other collateral to promote public awareness and educations which includes FAQs, Factsheets, an instructional video for users as well as briefing packs. IIS considers these efforts to be important in not only driving uptake but also in ensuring that Victorians are adequately informed about the DDL and its processes.

As noted, invitations to register for both products have been prepared and have recently gone live on the websites.

The DTP, the JVO, and Service Victoria will continue to build content to support business awareness of a DDL and how they could use it in practice, including the steps to validate the licence, identity or age cards. DTP is also working closely with VicPol on operational and technical needs.

In general, IIS considers the C&E Plan is taking a privacy and security friendly and focussed approach. Both issues are prominent in the discussion and approaches outlined. IIS has some observations about the Plan content, which it considers, if addressed in the further implementation work, will add to the clarity and accuracy of privacy messages.

Noting that the DTP, the JVO and Service Victoria are working on privacy materials, it also is important that there is a clear process for coordinating and approving the privacy materials across the DDL project. In addition, the privacy messages delivered by both DTP, JVO and Service Victoria should reflect the specifics of each app and, where appropriate, be consistent. IIS has addressed the coordination issue in Recommendation 1 above. It makes the following additional comments:

- The C&E plan alludes to, but does not specifically make clear, some of the key differences between the two apps, in particular, what information is shared with validators and whether or not an Internet connection is needed. Customers are encouraged to adopt whichever app is best for them but it will be more difficult for them to make an informed choice if the differences are not clear.
- The C&E plan and information about the DDL on both Service Victoria and VicRoads websites emphasise the privacy and security benefits of the DDL. IIS considers that it is important the benefits are not overstated, given, as IIS understands that there are still risks of fraud, misuse, or data breach. In the interests of transparency and helping DDL customers to protect themselves, IIS encourages the DTP and the JVO to develop security advice for customers, which is updated as any threats emerge.

---

<sup>10</sup> Communications and Engagement Plan April 2023

## 5. FINDINGS AND RECOMMENDATIONS

- The question of whether law enforcement bodies, or other validators, are able to request to hold a customer's device to view a DDL has been an issue in other jurisdictions. The C&E Plan does not currently provide advice on this for customers or validators. IIS understands that there will be no requirement for customers to hand over their devices. We consider this should be made clear to all parties.
- IIS also considers that it should be clear to customers that DDLs might not be accepted in all circumstances at least initially, including overseas. For example, validators might not take up the QR code scanning option, or they might need to take a copy of a licence. While it might be ok to 'leave your plastic in your pocket', it might be clearer to encourage customers to have the plastic card with them during the pilot period.<sup>11</sup> In addition, while IIS understands that customers do not need to have a licence with them, except where there is a legal requirement to carry, e.g. learners and probationary drivers, it might be helpful to make this clear.

The C&E Plan includes communications evaluation measures. For customers, the measure identified is an 'overall customer satisfaction score of >95%'. IIS understands the approach to measuring customer satisfaction is still being developed. We encourage the DTP to include privacy 'satisfaction' in the approach. This could include questions about whether customers has sufficient information to make an informed choice about using a DDL, and if they were confident that privacy and security would be protected.

### Recommendation 5 – Ensure DDL privacy and security information is accurate and does not overstate benefits.

Ensure that communications for the DDL pilot:

- Provide clear information about the differences between the JVO and the Service Victoria apps, in particular what information is shared with validators and whether or not an Internet connection is needed.
- Do not overstate the privacy and security benefits of the DDL, for example, by using unqualified language or not mentioning possible security risks.
- Make it clear that customers are not required to hand over their devices to law enforcement or other validators.
- Provide accurate advice about whether a plastic licence must be carried and the circumstances in which a plastic card might still need to be shown.

**Who:** Both the JVO and the DTP

**Timeframe:** For the external pilot and ongoing

<sup>11</sup> <https://www.vicroads.vic.gov.au/licences/digital-driver-licence/register> viewed 11 June 2023

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 6 – Include privacy in pilot evaluation.

Include privacy ‘satisfaction’ in the evaluation of pilot communications. Issues to consider could include understanding of the QR code content, whether customers had sufficient information to make an informed choice about using a DDL, and if they were confident that privacy and security would be protected.

**Who:** The DTP

**Timeframe:** For the external pilot

### 5.1.3 Security – IPP 4

IPP 4 requires agencies to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. The DTP and the JVO will also be subject to the VPDSF and VPDSS. The VPDSS prescribes a minimum set of mandatory requirements across all security areas including governance, information, personnel, ICT and physical security. The VPDSF provides direction to Victorian public sector agencies or bodies, or in the case of the JVO, brought in under s 84(3) of the PDPA, on their data security obligations.

As noted in the PIA scope ([Section 2.1](#)) the PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features.

The DTP has undertaken an Information Value Assessment (IVA) 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Factors taken into account include that:

- The DTP is sharing images and R&L data together, which it would usually only do in limited circumstances because of the sensitivity and high value of the data
- The potential volume of data to be shared with the JVO and Service Victoria
- The impact on public confidence and community safety if the integrity of drivers licence is impacted.

IIS has not validated this assessment as part of the PIA, but has not noted any issues.

#### 5.1.3.1 System security

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

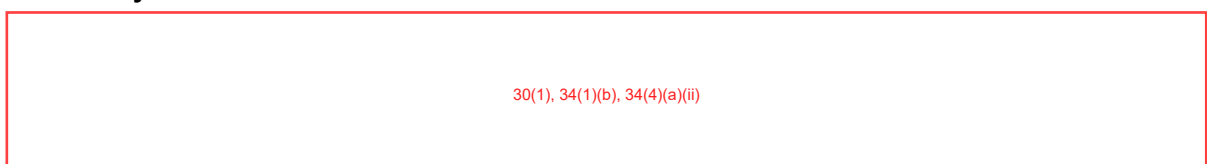
The JVO has noted a number of design features for the project that aim to mitigate the risks. It has also taken steps, including as required under the Deed, to manage its security approaches. The IVA and the protected designation require rigorous assessment of systems and processes to determine what more is needed. IIS understands that the JVO has addressed the security recommendations in the first Service Victoria DDL PIA.

Security actions that are relevant for this PIA include:

- **Incorporation of Security by Design in the development of the DDL**
  - The DDL has been designed with privacy and security recommendations from ISO 18013-5 in mind. The recommendations include: minimising data wherever possible; embedding privacy in design, flows, and architecture; keeping operations visible and transparent to the customer; designing for user-centricity and user control.



- **Security assessments**



## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Although IIS has not done a security assessment, we consider the security approach for the myVicRoads is likely to limit both privacy and security risks. It has not identified any issues of concern. However, if not already the case, it encourages the JVO to ensure that its security risk processes take account of risks to individuals.

### Recommendation 7 – Record DDL related privacy risks on the project risk register

Include privacy risks to individuals using a DDL in the risk register and ensure that these risks are continuously monitored.

**Who:** The JVO

**Timeframe:** Before full roll out

#### 5.1.3.2 Security for DDL customers

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(ii)

IIS agrees that a number of features of the JVO DDL appear to offer security advantages, possibly more than a plastic licence. These include:

- A DDL will quickly fail to display if the DTP has been notified that a licence has been lost or stolen.
- MFA is mandatory as part of setting up a DDL on a device, and when re-logging into a myVicRoads account.
- Data is updated regularly, meaning changes of address or licence conditions are easily refreshed.
- Customers can delete the DDL from their device.
- The inclusion of a card number on licences, which can be easily replicated on either the myVicRoads or Service Victoria app, depending on which is being used provides an additional element to protect identity in the event of a data breach.

30(1), 34(1)(b), 34(4)(a)(ii)

---

<sup>12</sup> <https://service.vic.gov.au/early-access/digital-driver-licence/home>

## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(i)

Overall, IIS has not identified any significant areas of concern from a privacy perspective with the JVO's security approach for the DDL. The approach seems consistent with privacy and security by design and is positive and comprehensive. Our recommendations identify areas where some additional steps could enhance the security response.



## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 8 – Continue to assess security risks for individuals and provide up-to-date information on risks and mitigations.

Continue to assess and monitor risks of identity fraud or other misuse of DDL that might pose risks to individuals. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Provide up to date information for customers on possible security risks and how to mitigate them.

**Who:** The JVO

**Timeframe:** For the full rollout and ongoing

### Recommendation 9 – Explore options for limiting address display on the DDL driver licence view.

Explore options for allowing differential display of address on the driver licence view.

**Who:** DTP and JVO

**Timeframe:** For the full roll out

### Recommendation 10 – Clarify requirements for the handling of individuals' devices for DDL validation.

Clarify whether validators may take an individual's device when checking a DDL, including if necessary, by considering legislative change.

**Who:** DTP

**Timeframe:** For the full roll out

## 5. FINDINGS AND RECOMMENDATIONS

### 5.2 Governance

#### 5.2.1 Project governance

While some development work remains, the DDL Project is now moving to its implementation phases, commencing with the external pilot in July. IIS has been impressed with the emphasis to date on both privacy and security by design in the design and built phases of the DDL. Strong privacy and security protective measures have been included.

However, IIS is less convinced about the more general privacy management for the project. In particular we note that:

- The Steering committee receives privacy reports and updates on privacy but does not have member with a direct privacy responsibility.
- Privacy notices have not yet been developed and the JVO seemed uncertain of the coordination and approval processes that might be needed given both DTP and Service Victoria will have an interest. IIS understands that the DTP will be encouraging consistency and will pointing to Service Victoria's privacy information as the standard, subject to differences in approach for the two apps. IIS considers standard information will be particularly relevant for the pilot. However, the ongoing operation for the myVicRoads app – where individuals sign up for the myVicRoads app via their myVicRoads account, and use of the myVicRoads app per se involves limited collection or sharing of personal information – means that the Service Victoria collection notices might not be directly applicable. Consistency, to the extent possible, between the collection notices for the two apps is preferable.
- There does not appear to be a governance process that would consider or monitor privacy approaches and issues across the three organisations that, for example, might arise in relation to privacy collection notices, privacy messages for the pilot or more generally, issues arising from the external pilot, or the handling of privacy complaints.
- The Deed requires the JVO to have a privacy management plan. IIS was advised that the plan is currently being developed. It is outside the scope of the PIA to comment on the JVO's privacy management more generally. However, IIS considers the privacy management plan could help ensure a coordinated best practice approach and for privacy to remain a priority in implementation, evaluation, and monitoring phases of the DDL.

IIS also notes that the JVO and the DTP have some shared responsibilities in the handling of customer enquiries and complaints including privacy complaints. These are subject to the Deed and to processes and work flows that will be developed. IIS understands these would also address any requests for access to or correction of personal information. The DTP will remain the responsible for requests relating to R&L data but there may be cases for the JVO or where there is a shared responsibility.

The JVO customer channels should guide customers to the appropriate source of help. However, given that Service Victoria is also offering DDLs there is a (possibly low) risk that customers will approach the wrong organisation to seek help or make a complaint. IIS encourages the organisations to ensure, via governance arrangements, that there are arrangements in place to ensure that there is 'no wrong door' and customers are directed and assisted to the right place.

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 11 – Strengthen DDL privacy governance arrangements including by relevant provisions in the JVO privacy management plan.

Identify or establish a process that will allow coordination and monitoring of privacy approaches relevant to the DTP, the JVO and Service Victoria. Ensure these processes are effective so that there is 'no wrong door' for requests for access and correct, or for lodging privacy complaints.

In completing the JVO privacy management plan, include strategies to ensure a coordinated best practice approach, and to ensure that privacy remains a priority in implementation, evaluation, and monitoring phases of the DDL.

**Who:** The JVO

**Timeframe:** For the full DDL roll out

### 5.2.2 Privacy by Design and future developments

As noted, PbD has been a feature of the DDL project development to date. In part, this has been driven by the JVO's customer first focus, recent data breaches and ISO and other international standards.

IIS encourages the JVO to continue this approach, which will clearly remain relevant as the DDL is implemented and as further enhancements are introduced. IIS understands these might include:

- 
- 
- 
- 
- DDLs available for learners and probationary permits
- Displaying the number of demerit points a person has accrued (preferably this would be displayed 'below the fold')
- Alerts or notifications that a learner permit and/or driver licence is due to expire, or that a future ban is about to commence.

IIS encourages the JVO to consider undertaking further PIAs at relevant points in the development process. It also encourages the JVO to consider if any additional processes, for example, via the privacy management plan, or governance arrangements, are needed to ensure the PbD approach continues to be strong feature of the JVO DDL.

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 12 – Take steps to ensure continued PbD approach in the DDL’s further development.

Continue the current PbD approach for the DDL, including by conducting further PIAs before making changes to the DDL, for example sharing licence information with validators, or introducing notifications, or display of status or demerit points, which could impact on individuals' privacy.

Ensure privacy management processes, such as the privacy management plan, or other project management or governance processes, are in place to ensure the PbD approach continues to be strong feature of the JVO DDL.

**Who:** The JVO

**Timeframe:** Full roll out and ongoing

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

6. APPENDIX A – METHODOLOGY

## 6. Appendix A – Methodology

### 6.1 PIA approach

IIS took the following steps to carry out the PIA:

- *Planning* with the DTP and JVO to confirm the approach, scope and deliverables of the PIA
- *Gathering information* by reading documents and meeting with personnel from the DTP and the JVO
- *Analysing the information* against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy good practice
- *Identifying privacy risks* and developing ways to mitigate those risks
- *Developing a preliminary findings note* summarising the key findings from the information gathering stage
- *Drafting the PIA report* and providing this to the DTP and JVO for comment
- *Finalising the PIA report* following feedback from the DTP and JVO.

### 6.2 Documents reviewed

Documents reviewed	
<b>DTP documents</b>	
1.	Communications and Engagement Plan April 2023
2.	Concession Deed, privacy <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>
3.	<span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>
4.	<span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>
5.	Department of Transport & Planning, Information Value Assessment
6.	<a href="#">DTP Privacy Policy</a>
7.	DTP Risk Matrix
8.	Establishing an identity with VicRoads
9.	Separation model, JVO and State
10.	Victorian Government Gazette, No. S 523, October 2022, application of PDPA to JVO

6. APPENDIX A – METHODOLOGY

Documents reviewed	
<b>The JVO documents</b>	
1.	30(1), 34(1)(b), 34(4)(a)(ii)
2.	30(1), 34(1)(b), 34(4)(a)(ii)
3.	myLearners T&C
4.	30(1), 34(1)(b), 34(4)(a)(ii)
5.	30(1), 34(1)(b), 34(4)(a)(ii)
6.	30(1), 34(1)(b), 34(4)(a)(ii)
7.	30(1), 34(1)(b), 34(4)(a)(ii)
8.	MyVicRoads T&C for use <a href="https://www.vicroads.vic.gov.au/website-terms/individual-terms-and-conditions">https://www.vicroads.vic.gov.au/website-terms/individual-terms-and-conditions</a>
9.	Privacy policy at <a href="https://www.vicroads.vic.gov.au/website-terms/privacy">https://www.vicroads.vic.gov.au/website-terms/privacy</a>
10.	Protecting Your Privacy Brochure (available from myVicRoads website, including by search or link in T&C)
11.	Rough scope of high-level assessment
12.	Service Victoria draft privacy collection notice (from May 2022 PIA)
13.	30(1), 34(1)(b), 34(4)(a)(ii)
<b>Relevant Service Victoria documents</b>	
1.	Draft Service Victoria Privacy Collection Notice for DDL pilot (May 2022)
2.	30(1), 34(1)(b), 34(4)(a)(ii)
3.	Service Victoria DDL FAQs <a href="https://service.vic.gov.au/early-access/digital-driver-licence/home">https://service.vic.gov.au/early-access/digital-driver-licence/home</a>

6. APPENDIX A – METHODOLOGY

### 6.3 Meetings held

Meetings held	Date
Kick-off meeting: <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP and JVO personnel</li> </ul>	23 May 2023
PIA information gathering meeting – <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> (JVO) and DTP: <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP and JVO personnel</li> </ul>	16 May 2023
PIA information gathering meeting – <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> (JVO): <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP and JVO personnel</li> </ul>	19 May 2023
PIA information gathering meeting – <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)</span> (JVO) <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP and JVO personnel</li> </ul>	22 May 2023
PIA information gathering meeting – <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> (JVO): <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP personnel</li> </ul>	23 May 2023
PIA progress update meeting: <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP and JVO personnel</li> </ul>	1 June 2023
PIA information gathering meeting – <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> <span style="border: 1px solid red; padding: 2px;">34(1)(b), 34(4)(a)</span> <ul style="list-style-type: none"> <li>IIS personnel</li> <li>JVO personnel</li> </ul>	7 June 2023
PIA progress update meeting: <ul style="list-style-type: none"> <li>IIS personnel</li> <li>the DTP and JVO personnel</li> </ul>	8 June 2023



## 7. Appendix B – Assessment against the IPPs

The following table sets out IIS's high-level assessment of the first release of the JVO DDL against the IPPs in the context of the external pilot and the expected full roll-out in 2024. This PIA focuses on the information flows for the myVicRoads app as described at [Section 3.5.3](#). The information flows between DTP, JVO and Service Victoria will be assessed in a separate PIA.

In making our assessment, we note that:

- The JVO app will display some health information in form of licence codes. This would be subject to the HPPs in the HRA. IIS notes that the HPPs cover similar issues to the IPPs and for this PIA has not undertaken a separate assessment.
- The JVO is handling R&L data on behalf of the DTP, which retains ownership of the data. The DTP continues to be responsible under privacy laws for the data. The JVO has specific privacy obligations under the Deed and separately is also directly subject to privacy laws.
- The JVO DDL approach (where data is displayed but not stored on an individual's device, and is not shared with validators (other than for law enforcement validation where driver licence number is contained in the bar code)) involves limited direct disclosure of personal information. However, the process would generally involve the individual in showing the DDL on their device to a validator. There is also a small, but not impossible, chance that data would be inadvertently disclosed if the device is subject to fraudulent misuse.

IIS also notes that where our assessment has not identified specific issues for this PIA, that is not meant to indicate there is no privacy work to be done. IIS anticipates that usual privacy compliance and monitoring would occur.

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 1 – Collection</b></p> <p>An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation’s Privacy Policy.</p>	<p>The DDL involves a re-use of existing information the DTP holds, not a new collection for DTP.</p> <p>Under the Deed, the JVO will be collecting and handling some personal information on behalf of the DTP.</p> <p>The introduction of DDL is a new way of providing driver licences – it would be at least good practice to update both the DTP’s and JVO’s privacy policies and to ensure privacy collection notices are available and relevant at point of use, for example within the myVicRoads app. The Deed states the Secretary must approve JVO collection notices and privacy policy. We also understand that the DTP policy intent is that the privacy information for the myVicRoads and Service Victoria apps will be consistent.</p> <p>See discussion at <a href="#">Section 5.1.1</a>.</p>
<p><b>IPP 2 – Use and disclosure</b></p> <p>Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual’s consent, for a law enforcement purpose, or to protect the safety of an individual or the public.</p>	<p>The DTP and JVO’s use of R&amp;L data for DDLs licence is consistent with the purpose of collection.</p> <p>Privacy law obligations, as well as the Deed, ensure that JVO must only use or disclose personal information as permitted under the Deed.</p> <p>In general, as noted above, the JVO is taking a cautious approach to disclosures of personal information for the myVicRoads app. <span style="border: 1px solid red; padding: 2px;">(1), 34(1)(b), 34(4)(a)</span></p> <div style="border: 1px solid red; padding: 10px; text-align: center; margin: 10px 0;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div> <p>No issues identified.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 3 – Data quality</b></p> <p>Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.</p>	<p>The DDL should not diminish and may enhance data accuracy of driver licence information.</p> <p>Changes to driver licence details or status will be subject to pilots and roll-out and will be reflected in the DDL quickly.</p> <p>The DTP’s requirements, and the JVO design are such the myVicRoads app does not collect or hold identified personal information. The one source of truth of driver licence information remains with the DTP. <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>  <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <p>No issues identified.</p>
<p><b>IPP 4 – Data security</b></p> <p>Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.</p>	<p>The DTP and JVO have in place detailed security management processes and have commenced or undertaken detailed security risk assessments for the DDL.</p> <p>At this point, there are some issues to work through – see discussion at <a href="#">Section 5.1.3</a>.</p>
<p><b>IPP 5 – Openness</b></p> <p>Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation’s Privacy Policy.</p>	<p>Both the DTP and the JVO have in place or will be updating or developing privacy policies, privacy notices and other privacy information. The intention is that the materials will be consistent and that individuals are easily able find relevant information to inform their decisions. IIS also considers that best practice would be to support more formal material with engaging, plain English information about DDLs and possible risks or issues.</p> <p>See <a href="#">Section 5.1.1</a> and <a href="#">Section 5.1.2</a></p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 6 – Access and correction</b></p> <p>Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982 (Vic).</p>	<p>The introduction of the DDL should not affect current processes for access and correction. However, JVO Service Victoria and the DTP should ensure respective responsibilities are clear and that processes are built with a ‘no wrong door’ approach.</p> <p>See <a href="#">Section 2.1</a></p>
<p><b>IPP 7 – Unique identifiers</b></p> <p>A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.</p>	<p>Driver Licence numbers are unique identifiers in terms of the PDPA.</p> <p>Driver licence numbers will appear on the DDL. However, the DDL project does not involve the assignment of new unique identifiers.</p> <p>No issues identified.</p>
<p><b>IPP 8 – Anonymity</b></p> <p>Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.</p>	<p>Not relevant for the DDL – identification is a required part of acquiring or using a DDL.</p>
<p><b>IPP 9 – Transborder data flows</b></p> <p>If an individual’s personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.</p>	<p>As far as IIS understands, the DDL processes are contained within Victoria.</p> <p>No issues identified.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 10 – Sensitive information</b></p> <p>The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.</p>	<p>Driver licence processes do not involve the collection of sensitive information as defined, but do involve some biometric and health information (See <a href="#">Section 3.6.2</a>). Such information is part of the R&amp;L data that the DTP has already collected.</p> <p>No issues identified.</p>

Released under the Freedom of Information Act 1982  
 Dept of Transport & Planning



Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

INFORMATION INTEGRITY SOLUTIONS PTY LTD

PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438

F: +61 2 9319 5754

E: [contact@iispartners.com](mailto:contact@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

ABN 78 107 611 898

ACN 107 611 898



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

**Report: 24 November 2023**

**Department of Transport and Planning (DTP)**

**OFFICIAL: Sensitive**

# PRIVACY IMPACT ASSESSMENT

## JVO DIGITAL DRIVER LICENCE PROJECT



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

## Contents

Glossary	1
1. Executive summary	2
1.1 IIS's overall view	3
1.2 Recommendations	4
2. Introduction	7
2.1 PIA scope	7
2.2 About this report	8
3. Project description	9
3.1 Background	9
3.2 Project objectives and scope	9
3.2.1 Objectives and expected benefits of the project	9
3.3 Project status	10
3.3.1 Completion of external pilot and pilot feedback	10
3.3.2 State-wide release	11
3.4 About the DDL	11
3.5 Participants in the DDL Project MVP	12
3.5.1 The Department of Transport and Planning	12
3.5.2 Joint Venture Operator	12
3.5.3 ), 34(1)(b), 34(4)(	13
3.5.4 Service Victoria	13
3.5.5 Checkers – Victoria Police	13
3.5.6 Checkers – other organisations	13
3.5.7 Victorian citizens using a DDL	14
3.6 Nature of systems and information flows	14
3.6.1 Key system components	14
3.6.2 Kinds of information involved	15
3.6.3 Overview of information flows	16
3.6.4 Product changes since pilot release	19
3.7 Legal framework	20
3.7.1 Victorian laws	20



CONTENTS

3.8	Project governance	21
4.	Approach to risk analysis	22
4.1	Inherent privacy risks	22
4.2	Positive privacy aspects	23
4.3	Residual privacy risk level	24
5.	Findings and recommendations	25
5.1	IPP issues or risks	25
5.1.1	Transparency – IPP 1 and IPP 5	25
5.1.2	Disclosure – IPP 2	32
5.1.3	Security – IPP 4	34
5.1.4	Access and correction – IPP 6, and privacy complaint handling	41
5.2	Governance	41
5.2.1	Project governance	41
5.2.2	Privacy by Design and future developments	42
5.3	Additional considerations – negative use cases	44
5.3.1	30(1), 34(1)(b), 34(4)(a)(ii)	44
5.3.2	Fraudulent use cases	46
6.	Appendix A – Methodology	49
6.1	PIA approach	49
6.2	Documents reviewed	49
6.3	Meetings held	51
7.	Appendix B – Assessment against the IPPs	52

## Glossary

Abbreviation or term	Expansion or definition
API	Application programming interface
(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
DTP	Department of Transport and Planning
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
IIS	IIS Partners and Information Integrity Solutions Pty Ltd
IPP	Information Privacy Principles in the PDPA
34(1)(b), 34(	30(1), 34(1)(b), 34(4)(a)(ii)
JVO	The DTP's Joint Venture Operator for VicRoads
MVP	Minimum Viable Product
OVIC	Office of the Victorian Information Commissioner
PDPA	<i>Privacy and Data Protection Act 2014</i>
PIA	Privacy Impact Assessment
QR Code	Quick Response Code
R&L	Registration & Licensing
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VicPol	Victoria Police

## 1. EXECUTIVE SUMMARY

# 1. Executive summary

The Department of Transport and Planning (DTP), its Joint Venture Operator VicRoads (JVO) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. A DDL will allow a licence holder to access an electronic version of their licence on a mobile device and present it in place of the physical licence. The DDL will be made available both through the myVicRoads and the Service Victoria platforms and apps.

The first phase of the DDL Project was producing a Minimum Viable Product (MVP), which replicated the data and attributes from the existing Victorian driver licence to a digital credential in either the myVicRoads app or the Service Victoria digital wallet. The second phase was testing the Minimum Marketable Product (MMP) via an external regional pilot in Ballarat, which commenced in July 2023. The agencies are now working towards a state-wide release of the DDL, starting in 2024.

The current DDL solution focuses on three primary use cases:

- Entitlement to drive
- Proof of identity (i.e., the customer's name and address)
- Proof of age (i.e., the customer is over 18).

The DDL products draw on the JVO's driver licence registry, which contains the DTP's holding of registration and licencing (R&L) data, and which it operates on behalf of the DTP. The quantity and sensitivity of personal information involved means the privacy impacts of the DDL Project need to be carefully examined.

IIS Partners (IIS) had previously conducted two Privacy Impact Assessments (PIAs) on the first phase of the DDL Project (prior to the external pilot) – one for Service Victoria and one for the JVO. This PIA report, which focuses on the JVO DDL solution, is an update of the initial PIA (dated June 2023), taking into account JVO's roles in delivering the DDL project for the state-wide release. A separate report will update the June 2023 PIA of Service Victoria's implementation of the DDL.

The scope of the PIA covers privacy risks associated with:

- The back-end integration to the driver licence registry, including APIs, for both products
- The design and build of the myVicRoads app
- Data flows between the JVO and the myVicRoads app
- Security of the information
- Onboarding and user experience in the myVicRoads app
- Features and use cases within the initial release scope
- Any product changes made to the DDL since the pilot
- Core privacy requirements under the Information Privacy Principles (IPPs)

## 1. EXECUTIVE SUMMARY

- Potential negative use cases and mechanisms to address them.

In undertaking this PIA, IIS considered:

- Privacy principles in the *Privacy and Data Protection Act 2014*
- The Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS)
- Relevant legislation such as *Road Safety Act 1986* and the *Service Victoria Act 2018*
- Guidance materials published by the Office of the Victorian Information Commissioner (OVIC) and the Office of the Australian Information Commissioner (CAIC)
- Privacy good practice stemming from IIS's knowledge and experience.

This report:

- Provides background to the project, including key project participants and roles, key systems and information flows, and the relevant legal framework.
- Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

The PIA methodology is included in the Appendices.

### 1.1 IIS's overall view

Privacy and security have been a key focus for the JVO in project design and implementation. IIS has not identified any high-risk privacy issues for the project with respect to implementation of appropriate controls to manage the inherent high risks. Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. The issues identified arise in the context of the project stage, which is now turning to implementation and the full-roll out, and the complexity of the project environment.

30(1), 34(1)(b), 34(4)(a)(ii)

- There is significant quantity and sensitivity of personal information involved.
- The project will involve the display of R&L data in DDLs via individuals' devices.
- The data involved includes sensitive biometrics, like driver images as well as R&L details.
- The DDL project environment is complex, with both the JVO and Service Victoria offering DDL credentials via their respective apps, under the guidance of the DTP. The apps while developed independently are expected to meet the DTP's policy and Design Standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- The JVO design aims to take account of possible security risks for DDL users. However, these risks will need to be monitored on an ongoing basis.

## 1. EXECUTIVE SUMMARY

- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including the differences in the two apps, or how verifiers can interact with their devices, or handle personal information shared or displayed via the DDL – could cause concern and jeopardise uptake of the solution.

Overall, the DDL has benefited from being designed in a privacy-friendly way. Taking into account the positive privacy aspects such as the emphasis on data minimisation, the avoidance of a new digital footprint, the DDL security features, and expected detailed governance arrangements, we consider that the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, the development of privacy coordination and monitoring arrangements, and close attention to the possible security risks for customers using a DDL.

In our previous June 2023 PIA, IIS identified key privacy risks and issues in the following areas:

- Transparency and privacy complaint handling
- Security
- Privacy governance.

IIS has retained our analysis in relation to the abovementioned areas and added to the analysis any updated information that we have received from JVO and the DTP.

### 1.2 Recommendations

IIS made a total of 12 recommendations in our previous PIA. Since then we note that JVO and the DTP have implemented a number of our recommendations. The status of implementation is displayed in the table below. For this PIA, IIS has a further 10 recommendations for the JVO and the DTP's consideration as it continues to rollout the DDL state-wide. For your ease of reference, the recommendations for this PIA have been listed as Recommendation A, B, C and so forth.

#### Status of previous recommendations

Recommendations	Who	Status
<b>Recommendation 1</b> – Project governance processes to ensure consistent, best practice privacy messages for both the myVicRoads and Service Victoria apps	JVO, DTP & Service Victoria	Implemented
<b>Recommendation 2</b> – Privacy information about the DDL pilot to be prominent and easily accessible	JVO & DTP	Retained – see <b>Recommendation A</b>
<b>Recommendation 3</b> – Pilot collection notices to use plain English and be supported by an overview of the DDL	JVO & DTP	Implemented

## 1. EXECUTIVE SUMMARY

Recommendations	Who	Status
<b>Recommendation 4</b> – The JVO privacy policy to include comprehensive DDL information	JVO & DTP	Retained – see <b>Recommendation B</b>
<b>Recommendation 5</b> – Ensure DDL privacy and security information is accurate and does not overstate benefits	JVO & DTP	Retained – see <b>Recommendation C</b>
<b>Recommendation 6</b> – Include privacy issues in pilot evaluation	JVO & DTP	Implemented
<b>Recommendation 7</b> – Record DDL related privacy risks on risk register	JVO	Implemented
<b>Recommendation 8</b> – Continue to assess security risks for individuals and provide up-to-date information on risks and mitigations	JVO & DTP	Implemented
<b>Recommendation 9</b> – Explore options for limiting address display on the DDL driver licence view	JVO & DTP	Implemented
<b>Recommendation 10</b> – Clarify requirements for the handling of individuals’ devices for DDL validation	DTP	Implemented
<b>Recommendation 11</b> – Strengthen DDL privacy governance arrangements including by relevant provisions in the JVO Privacy Management Plan	JVO	Retained – see <b>Recommendation G</b>
<b>Recommendation 12</b> – Ensure continued PbD approach in the DDL’s further development	JVO	Implemented

### New / retained recommendations

Recommendations	Who	Timeframe
<b>Recommendation A</b> – Make privacy-related information about the DDL prominent and easily accessible	JVO & DTP	State-wide release and ongoing

1. EXECUTIVE SUMMARY

Recommendations	Who	Timeframe
<b>Recommendation B</b> – JVO’s privacy policy to include or link to comprehensive DDL information	JVO & DTP	State-wide release and ongoing
<b>Recommendation C</b> – Ensure DDL communications, including privacy and security information, are accurate, consistent and fit-for-purpose	JVO & DTP	State-wide release and ongoing
<b>Recommendation D</b> – Continue to support engagement with businesses during state-wide release	DTP, JVO & Service Victoria	State-wide release and ongoing
<b>Recommendation E</b> – Continue to monitor customer feedback	DTP, JVO & Service Victoria	State-wide release and ongoing
<b>Recommendation F</b> – Monitor the effectiveness of the processes when engaging the DTP Vulnerable Customers Team	JVO	Ongoing
<b>Recommendation G</b> – Strengthen DDL privacy governance arrangements including by relevant provisions in the JVO privacy management plan	JVO	For post ‘Delivery’ mode
<b>Recommendation H</b> – Communicate to <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> on the importance of keeping their personal details updated	JVO & DTP	Ongoing
<b>Recommendation I</b> – Consult with DTP Vulnerable Customer Team and other relevant <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>	JVO & DTP	Ongoing
<b>Recommendation J</b> – Review current materials for licence checkers to identify if more guidance is needed to mitigate against potential fraud cases	JVO & DTP	Within 3-6 months of initial state-wide rollout

## 2. Introduction

The Department of Transport and Planning (DTP), its Joint Venture Operator for VicRoads (JVO) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. The DDL will be made available both through the myVicRoads and the Service Victoria platforms and apps.

Both the products will leverage data from VicRoads Driver Licence registry, currently operated by the JVO on behalf of DTP. Both products have integration with DTP's driver licence registry using the new technical integration framework that the JVO is implementing as part of the DDL program. DTP provides policy oversight and guidance to ensure that the DDL products are aligned in key areas to deliver a consistent user experience to Victorian motorists.

IIS had previously conducted two PIAs on the first phase of the DDL Project -- the first for the MVP for the internal pilot (June 2022) and the second for the MMP for the external pilot in Ballarat. This PIA report is an update from the previous MMP PIA (dated June 2023), taking into account JVO's roles in delivering the DDL project for the state-wide release in 2024. A separate report will update the June 2023 PIA of Service Victoria's implementation of the DDL.

### 2.1 PIA scope

30(1), 34(1)(b), 34(4)(a)(ii)

The first phase of the DDL Project was producing an MVP which replicates the data and attributes from the existing Victorian driver licence to a digital credential in either the myVicRoads app or the Service Victoria digital wallet. The first release was tested through an external pilot that took place in Ballarat, which commenced in July 2023. There have been certain changes to the DDL since the external pilot.

This version of the PIA is an update to the previous PIA which covers JVO's delivery of the APIs, 34(1)(b), 34(4)

30(1), 34(1)(b), 34(4)(a)(ii)

and additionally include the assessment of any changes or development made to the DDL post external pilot release that may affect privacy compliance and introduce new privacy risks.

The scope of this PIA will include the following additional developments:

- DDL product changes
  - 30(1), 34(1)(b), 34(4)(a)(ii)
  - Channel limiting (allowing only 2 instances of a person's credential via each channel)
- Updates to privacy policies, websites and communications .



## 2. INTRODUCTION

The PIA will also discuss potential negative uses of the DDL as well as consider any risks/issues in anticipation of the planned state-wide rollout in 2024.

30(1), 34(1)(b), 34(4)(a)(ii)

In providing this report, IIS makes the following qualifications:

- The PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features.
- The PIA is based on information gathered from, and provided by, the DTP and the JVO.
- IIS does not provide legal advice; rather we provide strategic privacy and cyber security advice.

### 2.2 About this report

The report is structured to provide an overview of the DDL project, explain IIS's approach to risk analysis, analyse privacy issues according to the project scope, and provide additional context to the PIA work:

- **Project description** ([Section 3](#))  
Provides background to the DDL Project, key project participants and roles, key systems and information flows, and the relevant legal framework.
- **Approach to risk analysis** ([Section 4](#))  
Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- **Findings and recommendations** ([Section 5](#))  
Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.
- **Appendix A – Methodology** ([Section 6](#))  
Summarises our methodology, including list of documents reviewed and meetings held.
- **Appendix B – High-level assessment against the Information Privacy Principles** ([Section 7](#))  
Provides a high-level assessment of the DDL project against the IPPs and notes risks areas, which are discussed in detail in [Section 5](#).

### 3. PROJECT DESCRIPTION

## 3. Project description

### 3.1 Background

The DTP, JVO and Service Victoria are working to bring DDLs to Victorian residents. Digital licences offer customers a convenient and secure means to present a driver licence or have their proof of age or identity details verified, where they are required to do so. Three out of six Australian state and territory jurisdictions have either trialled or have a legislation-based DDL. According to Service Victoria research, six million Victorians possess a driver licence and 80% of the licence holders would value a digital driver's licence.

The DDL replicates data and attributes from an existing plastic Victorian driver licence to a digital credential. Initially there will be three primary use cases:

- Entitlement to drive whilst on the road.
- Casual proof of that user is over 18 and photo for licensed venues and businesses such as supermarkets, convenient stores, tobacco retailers, etc.
- Proof of identity (comprising a customer's name and address).

It will be up to the businesses and organisations who are relying parties to decide whether or not to accept the DDL for these use cases.<sup>1</sup>

The DDL products support verifications where the information is presented on various DDL views using QR code scanning (using the myVicRoads or Service Victoria apps). This feature enables individual and business customers to verify the details presented by a DDL holder without requiring specialised hardware or facial recognition.

A first release of the DDL came in the form of an external pilot which commenced in July 2023. The DTP, JVO and Service Victoria are now working towards a state-wide release, planned for 2024. At this stage, the DDL will be supplementary to the physical driver licence and will not replace it. While most full licence drivers do not need to carry a physical licence, where the existing laws do require this, they remain enforceable. For example, the introduction of DDLs does not change the obligation of motorists such as learner and probationary drivers to always carry their physical licence with them.

### 3.2 Project objectives and scope

#### 3.2.1 Objectives and expected benefits of the project

The DDL is consistent with the Victorian Government's digital strategy, which is expected to deliver cost savings, and better, fairer, and more accessible services, and a digital ready economy.

---

<sup>1</sup> There will be circumstances where a DDL will not be sufficient and a physical driver licence DDL might be needed. For example, the first state-wide release will not allow a business to easily retain a copy of DDL ID details as part of their existing legal or operational requirements.

### 3. PROJECT DESCRIPTION

The expected benefits of the DDL for Victorian drivers are:

- Freedom – As noted, unless required to by law, most customers will be able to leave their physical licence and wallet at home (although they might still need a plastic licence, for example, to prove identity in some circumstances).
- Peace of mind – Customers know their DDL is always on their phone as a backup.
- Convenience – 89% of the customers Service Victoria consulted indicated that they believe the DDL to be more convenient than a physical driver licence because they always carry their phone with them.
- Security – No personal information is stored on the customer's device, and setup of the myVicRoads app includes multi-factor authentication (MFA) and requires a user login, and a six-digit PIN or biometric.
- Privacy – Customers will have a choice of how to display the DDL on their device depending on the use case (entitlement to drive, proof of age, proof of ID). If a verifier seeks to confirm details displayed on the device via the QR, no personal information, other than licence number on the licence view, is shared. The QR code only confirms the details are correct or provides various limited error codes if for some reason the information cannot be verified.
- Up-to-date data management – Customers using a DDL have access to up-to-date information about the status of their licence; for example, whether it is valid or has expired.

### 3.3 Project status

The DTP, JVO and Service Victoria are taking an iterative approach to the DDL project. JVO and the DTP have undertaken significant development work since the initial MVP in 2022. The design and build of the JVO DDL are complete.

#### 3.3.1 Completion of external pilot and pilot feedback

The external pilot started in July 2023 in Ballarat. JVO and Service Victoria promoted the pilot via their websites. The JVO sent out email invitations to its customers in the Ballarat area, requesting their participation. Service Victoria on the other hand asked people to sign up, checked to ensure that there was no duplicate between Service Victoria and JVO and only sent out invitations specifically to those people. At the time of this PIA, there were approximately 11,000 active Victorian DDLs across both channels.

Both Service Victoria and JVO reported that they received positive feedback on the DDL, with no negative feedback about the product itself. [Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

The JVO in particular has planned to release a survey that will go out to users to gain their feedback, including on how well the DDL protects privacy and personal information as well as general feedback on how to improve the DDL. This is discussed in [Section 5.1.2](#).

### 3. PROJECT DESCRIPTION

#### 3.3.2 State-wide release

The project is now moving towards state-wide release in 2024. IIS has not identified any crucial issues that needs to be addressed prior to the state-wide release. Our recommendations are not time sensitive and should be considered by JVO and the DTP in their future planning of the DDL.

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.4 About the DDL

The DDL is the first product in the myVicRoads app and will be available through the myVicRoads portal. DDL customers will be able to easily show an identical digital version of their driver licence, and to have certain details verified, via their myVicRoads app. Initially, the DDL can be used in three cases:

- Entitlement to drive
- Proof of identity
- Verification that the customer is over 18.

The DDL acts in a similar fashion to a physical licence. However, some details can be hidden by default to respect the user's privacy. The DDL effectively contains three cards. The myVicRoads app landing screen provides customers with the opportunity to select the digital card that best suits the context. The customer can show and verify subsets of their DDL details. For example, a verifier scanning an age card, only sees the fact they're over 18, rather than their exact birthdate, driver licence number, address and other information, which is all apparent on a physical licence.

To set up a myVicRoads DDL, customers must first have a myVicRoads account

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

. DDLs are further protected by the customer's phone password (if used) and are only accessible by logging into the myVicRoads app via a user login, biometric identification, or six-digit PIN, and an additional authentication step (multi-factor authentication (MFA)).

The JVO has taken a cautious approach to privacy and security in the development of the DDL.

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

This means that personal information will be displayed on a customer's device when they activate the app but no personal information will be stored on the device. The verifier will still, with the customer's permission, be able to view the image and the details the customer chooses to display on the device.

The DDL will contain features such as holograms, manual refresh, display of the last refreshed date and time and a watermark, that are digitally equivalent to the features that indicate a plastic licence is legitimate. The DDL will also include a QR code that verifiers (organisations seeking to rely on a DDL) can scan to verify the licence is valid. The scan displays a green tick for valid cards or an error message (for example, QR code expired, invalid QR code). This is currently being updated to align with Service Victoria's solution. The DDL also contains a bar code, which contains only the customer's licence number, for Victoria Police (VicPol) use.

### 3. PROJECT DESCRIPTION

IIS considers that both the JVO and Service Victoria products have been designed and implemented with emphasis on data security and privacy (privacy and security by design). The DTP will also ensure the digital driver licence experience, design, functionality and features will be same across both DDL channels.

A customer may choose to have both the Service Victoria and myVicRoads apps on their device, from which they can access the DDL. [redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

[redacted]  
30(1), 34(1)(b), 34(4)(a)(ii)

At this point, the products are not interoperable [redacted]. This means that the JVO QR code can only be scanned with the JVO app and vice versa with the Service Victoria app.

30(1), 34(1)(b), 34(4)(a)(ii)

### 3.5 Participants in the DDL Project MVP

This section sets out the participants in the DDL project.

#### 3.5.1 The Department of Transport and Planning

The DTP operates and coordinates Victoria's transport network, the delivery and upgrade of transport infrastructure, as well as the reforms to road safety policy, regulatory and legislative environment. The DTP will remain the owner of the R&L data.

The DTP is also the policy owner of driver licensing policy. All the elements that relate to licence information, entitlement to drive, safety and roads will remain with the DTP. The user's licence features and potential changes (e.g., addition of a licence, expiration, suspension) are managed on the DTP's side, and JVO and Service Victoria only reflect those changes through the DDL.

The DTP provides policy oversight and guidance to ensure that the DDL products are aligned in key areas to deliver a consistent user experience to Victorian motorists.

#### 3.5.2 Joint Venture Operator

The JVO provides registration and licensing services under a Concession Deed (the Deed) on behalf of the DTP and VicRoads. In summary, it is responsible for customer service and operational activities

[redacted]  
30(1), 34(1)(b), 34(4)(a)(ii)

initial customer complaints, and management of the IT systems.

### 3. PROJECT DESCRIPTION

[Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii) The APIs will allow near-real time driver licence data to be retrieved by the front-end mobile apps developed by the JVO and Service Victoria.

The JVO is also responsible for the DDL solution design and build and will host the DDL in the myVicRoads app on the myVicRoads portal. It is responsible for the maintenance of the app and, subject to the Deed and the DTP policy and Design Standards, for ensuring that the right security, privacy and compliance features are in place. The JVO is also responsible for the communications with customers and will provide a digital channel for customer feedback about the DDL and pass complaints in relation to the DDL to the DTP.

#### 3.5.3 [Redacted]

[Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.5.4 Service Victoria

Service Victoria will, as noted, be a supplier of the DDL through its own channel. [Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

[Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.5.5 Checkers – Victoria Police

VicPol is a key stakeholder for the DDL and is working with DTP to identify and resolve any issues.

The external regional pilot was used to test the efficacy of, and seek feedback on, the VicPol app already available to check the barcode, which IIS understands contains only the licence number. VicPol only checks the DDL as an initial check. [Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

[Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

IIS understands that no issues were raised VicPol during the pilot and that they were generally pleased with the ease of using the solution. The DTP will continue to engage with VicPol to identify any needed modifications of police processes if/when the DDL becomes a replacement for a hard copy driver licence.

#### 3.5.6 Checkers – other organisations

There will be a number of businesses that need to verify licences or identification. These include:

- National Retailers Licensed venues such as bars, pubs, nightclubs and restaurants
- Hotels
- Petrol service stations

### 3. PROJECT DESCRIPTION

- Supermarkets and grocery stores
- Convenience stores
- Tobacco retailers
- Pharmacies
- Banks
- Australia Post
- Licensed premises, parcel pickup and delivery businesses, retailers offering click and collect, credit options and equipment hire.

IIS notes that the initial focus will be on small businesses that do not need to retain documentary evidence of identity. Such requirements might be considered in further iterations of the DDL.

#### 3.5.7 Victorian citizens using a DDL

At the time of writing, there were approximately 11,000 active Victorian DDLs across both the Service Victoria and JVO channels. The current DDL solution is only available for drivers with a full licence including car, motorcycle, light, heavy vehicles. The state-wide release is planned for 2024.

The DTP expects the DDL will be extended to all licence holders including probationary drivers and learner drivers in further stages of the project.

## 3.6 Nature of systems and information flows

### 3.6.1 Key system components

#### 3.6.1.1 The DTP

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.6.1.2 JVO

30(1), 34(1)(b), 34(4)(a)(ii)

### 3. PROJECT DESCRIPTION

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.6.1.3 Licence holders

Licence holders will use their own devices to set up, or use, a myVicRoads account, and to add a DDL to the myVicRoads app.

### 3.6.2 Kinds of information involved

#### 3.6.2.1 Personal information

The kinds of personal information JVO will display on the DDL is the same as that which currently appears on the plastic licence. As outlined, not all the information will be displaced for all views. The full set of personal information is:

- Full name
- Date of birth
- Address
- Signature
- Photo
- Licence number
- Licence expiry date
- Licence type (car/bike/dual)
- Licence proficiency (full/probationary)
- Licence category (heavy vehicle categories)
- Licence conditions
- Card Number (if allocated)
- Issue Date
- Licence Status.



### 3. PROJECT DESCRIPTION

#### 3.6.2.2 Sensitive information and health information

The DTP will also share conditions included on driver licences (e.g., alcohol interlock device, driver aids or vehicle modifications, etc.). One of the conditions is a letter 'S' that indicates glasses or corrective lenses. IIS considers that in this limited circumstance, the condition could meet the definition of health information in the *Health Records Act 2001*, although practically speaking the privacy risk is low.

The JVO DDL will also display biometric information in the form of the licence photo and signature. Biometric information is not currently explicitly contained in the definition of sensitive information in the *Privacy and Data Protection Act 2014*. However, it is considered sensitive information under the *Privacy Act 1988* (Cth) and OVIC advises organisations to consider treating biometric information as 'delicate information' and to handle it cautiously.<sup>2 3</sup>

#### 3.6.3 Overview of information flows

At a high level, the arrangements for the JVO DDL are expected to involve the following:

- [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)  
[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
- [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)  
[Redacted] 34(1)(b), 34(4)
- Customers who decide to opt in for a DDL are required to sign-up for a myVicRoads account and login using the in-app workflows provided by the mobile app. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)  
[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)  
[Redacted] 34(1)(b), 34(4)
- [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)  
[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii) The purpose of QR code to verify licence details are accurate as per the registry. When the app is 'activated', DDL information and images are retrieved using QR code [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii) and displayed on device.
- Customers can choose to show their DDLs to verifiers (law enforcement agencies, or businesses seeking proof of identity or age).
- Verifiers can also scan the QR code which will return a confirmation screen.
- VicPol can scan the barcode, which contains the licence number, and this comes up with licence number.

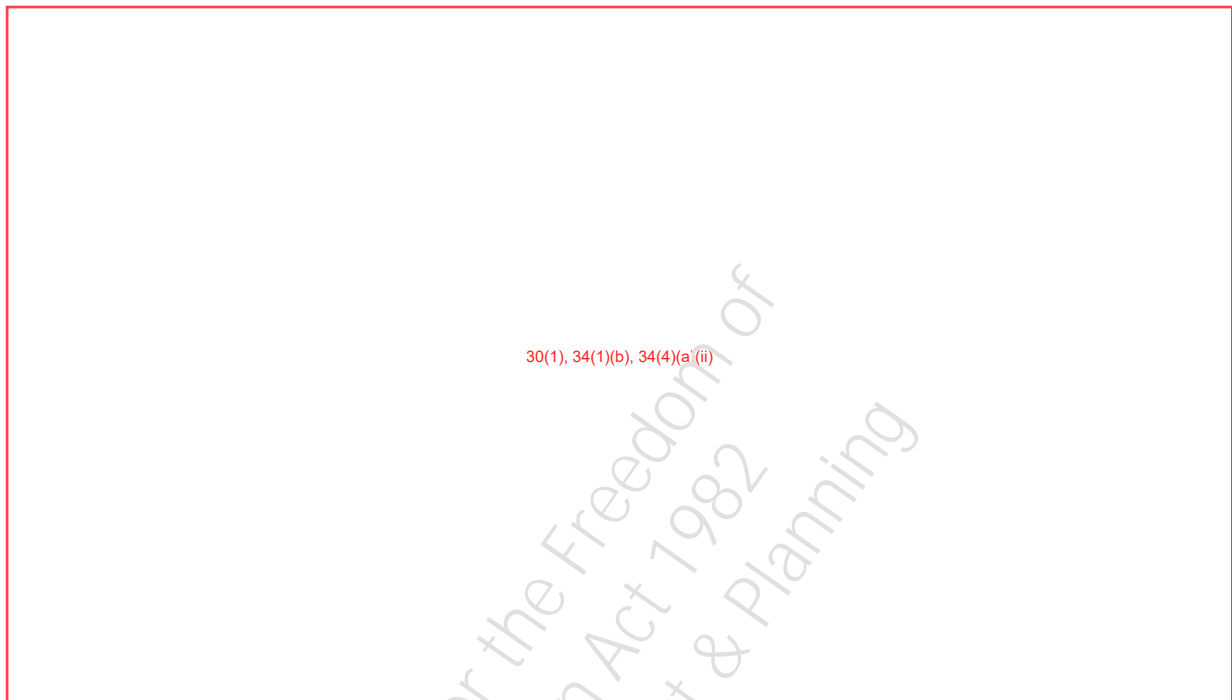
The following diagram provides an overview of the DDL architecture.

<sup>2</sup> Please refer to the definition given by OVIC: "Delicate information' refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regard as requiring a higher degree of protection.", available at [https://ovic.vic.gov.au/book/key-concepts/#Sensitive\\_and\\_delicate\\_information](https://ovic.vic.gov.au/book/key-concepts/#Sensitive_and_delicate_information)

<sup>3</sup> See <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>

### 3. PROJECT DESCRIPTION

Diagram 1 – Solution overview – JVO DDL



The table below sets out the expected information flows for the creation of a DDL in the myVicRoads app. It also describes the information flows when a QR Code is generated and verified using the myVicRoads app (both by the customer and the verifier).

Steps for the user	Back-end processes
<p>Log into the app / create an account</p> <p>The customer must first have, or set up, a myVicRoads account, <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <p><span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <p><span style="border: 1px solid red; padding: 2px;">34(1)(b), 34(</span></p> <p>The path to the DDL is via the myVicRoads portal – it is relying on established identities.</p> <p>When they have a myVicRoads account the customer would download the myVicRoads app and login.</p>	<p>The process of setting up a myVicRoads account is outside the scope of the PIA.</p> <p>If an account is created, email address and mobile phone (if provided) are verified via the use of a one-time passcode. <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <p><span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p>

3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
	<p style="text-align: center;">30(1), 34(1)(b), 34(4)(a)(ii)</p>
<p>Linking customer record to licence</p>	
<p style="text-align: center;">30(1), 34(1)(b), 34(4)(a)(ii)</p>	<p style="text-align: center;">30(1), 34(1)(b), 34(4)(a)(ii)</p>
<p>Adding the DDL to the wallet</p>	
<p>The customer can now access the DDL from the JVO app.</p>	

### 3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
QR Code generation and verification	
<p><b>Generating a QR Code:</b></p> <p>The user will be given the choice to decide on different sharing options. This will allow them to determine how much of their driver licence information they'd like to show to non-law enforcement verifier.</p>	<p>As noted, the JVO is not storing any personal information on mobile device. <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <div style="border: 1px solid red; height: 150px; width: 100%; margin-top: 10px;"> <p style="text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
<p><b>Verifying a QR Code:</b></p> <p>Businesses that require proof of age, proof of ID, or proof of eligibility to drive will be able to scan the QR code to verify its validity and the validity of the details in question.</p> <p>Law enforcement agencies checking licences will focus on licence number. The DDL will contain a barcode that contains the licence number.</p>	<div style="border: 1px solid red; height: 250px; width: 100%; margin-top: 10px;"> <p style="text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>

#### 3.6.4 Product changes since pilot release

30(1), 34(1)(b), 34(4)(a)(ii)

### 3. PROJECT DESCRIPTION

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

## 3.7 Legal framework

### 3.7.1 Victorian laws

The DDL project must comply with the following relevant laws.

#### 3.7.1.1 Privacy and Data Protection Act 2014

The *Privacy and Data Protection Act 2014* (PDPA) regulates the handling and protection of personal information by Victorian public sector organisations. Organisations subject to the PDPA must comply with the IPPs that contain requirements across the information lifecycle. Part 4 of the PDPA gives the Victorian Information Commissioner the power to prescribe security requirements pertaining to public sector information and information systems through the Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS).

Section 84(3) of the PDPA provides for organisations to be declared subject to the PDPA. Gazette S523 4/10/22 declares the JVO to be a body to which Part 4 of the PDPA applies.

#### 3.7.1.2 Health Records Act 2001

The *Health Records Act 2001* (HRA) and its Health Privacy Principles (HPPs) regulate the collection, handling and protection of health information, which includes information or opinion about the physical or mental health or disability of an individual.<sup>4</sup>

#### 3.7.1.3 Road Safety Act 1986

The *Road Safety Act 1986* (RSA) is the main piece of legislation that regulates the use of roads, registration of vehicles and driver licensing in Victoria.

---

<sup>4</sup> The HPPs are substantially similar to the IPPs. For the purposes of our privacy analysis in Section 5, IIS has focused on the IPPs.

### 3. PROJECT DESCRIPTION

Part 7B contains the protective framework for R&L information, including the allowed purposes for use and disclosure of relevant information, the exceptional circumstances for the use and disclosure of relevant information, the uses of relevant information for verification purposes, etc

#### 3.7.1.4 Charter of Human Rights and Responsibilities Act 2006

The *Charter of Human Rights and Responsibilities Act 2006* (the Charter) is a Victorian law that sets out the protected rights of all people in Victoria as well as the corresponding obligations on the Victorian Government. The DTP will be conducting a Charter assessment with particular focus on engagement or limitation of the right to privacy.

#### 3.7.1.5 Road Safety (Drivers) Regulations 2019

Regulation 63 of the Road Safety (Drivers) Regulations 2019 describes the details that driver licence or learner permit documents must contain, including the identification number, the person's first name, second and third initials (if any) and family name; a photograph of the person; the person's residential address; the person's date of birth; a reproduction of the person's signature; the category or categories of driver licence; its expiry date; and the code of any condition to which the licence or permit is subject.

### 3.8 Project governance

The project governance arrangements take account of the fact that the JVO is providing services to the DTP under a Concession Deed (the Deed), and the DDL project is authorised by Cabinet. The Deed sets out the JVO's and DTP's role and obligations, including for privacy and security. The DTP is effectively the regulator of the JVO under the Deed. The formal governance arrangements include:

- Ministerial oversight via monthly ministerial meetings
- Steering committee with senior staff from the DTP and Service Victoria
- Working groups sitting under the steering committee with weekly meetings; the JVO participates in relevant working groups (but not the steering committee).

## 4. APPROACH TO RISK ANALYSIS

### 4. Approach to risk analysis

In undertaking this PIA, IIS considered:

- The IPPs in the PDPA
- Guidance materials published by the OVIC and the OAIC
- Privacy good practice stemming from IIS's knowledge and experience.

The PIA focuses on privacy risks that are introduced or heightened by the DDL Project, rather than privacy risks for existing processes to issue and use driver licences.

This section assesses the project's residual privacy risk level, by weighing the inherent privacy risks against the existing privacy positive aspects.

The following section discusses the project's privacy issues and risks identified in detail and makes recommendations to mitigate the risks.

#### 4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks. Inherent privacy risks arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential (including value) for, and consequences of, misuse
- The range of people from whom the information may be collected
- The context in which personal information is handled – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the project
- The extent to which information is accessed or handled by third parties
- The likely community and/or media interest in the privacy aspects of the project.

30(1), 34(1)(b), 34(4)(a)(ii)

- There is significant quantity and sensitivity of personal involved.
- The project will increase likelihood of potential exposure of sensitive personal information data to the Internet via apps and APIs.
- The project will involve the display of R&L data in DDLs via individuals' devices.
- The data involved includes driver images as well as R&L details.

## 4. APPROACH TO RISK ANALYSIS

- The DDL project environment is complex, with both the JVO and Service Victoria offering DDL credentials via their respective apps, under the guidance of the DTP. The apps while developed independently are expected to meet the DTP's policy and Design Standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- The JVO design aims to take account of possible security risks for DDL users. However, there is still potential for risks to be greater than expected or for unforeseen risks to arise and so calls for a need for risks to be monitored on an ongoing basis.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including the differences in the two channels, or how verifiers can interact with their devices, or handle personal information shared or displayed via the DDL – could cause concern and jeopardise uptake of the solution.

### 4.2 Positive privacy aspects

IIS considers that the DDL Project has important positive aspects that support privacy and minimise the inherent risks associated with the project. These are outlined below:

#### Positive privacy aspects with the project/solution design

- The JVO has followed the key privacy enhancing strategy of data minimisation – there will be minimal personal information transferred to display on the customer's device and data is retrieved afresh and displayed each time a customer uses the device; no personal information is stored on the device. There is no persistence of data in the networks, and data is encrypted at all stages, from the APIs, onto the app.
- The DDL project design appears to avoid the risk of a new digital footprint, in that neither the JVO or the DTP will have any detailed records that would enable them to track when, or to whom, a customer presents their DDL for checking. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)
- 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) This means the DTP data remains the single 'source of truth' for driver licence information.
- The device does not retain any DDL personal information on the device, it is only displayed. Each time a customer uses or refreshes the DDL, the relevant information is retrieved from the server. When a QR Code is scanned, it requests a verification of the licence and its data from the VicRoads servers, and a response is returned, which confirms but does not provide the details on the licence. The QR code is generated by a call to the DTP, and, following verification, is only available for display without refresh for two minutes.
- JVO and DTP express a strong commitment to privacy and privacy appears to have been in mind throughout project design and for the implementation.



## 4. APPROACH TO RISK ANALYSIS

- The arrangement between DTP and JVO are governed by privacy legislation and by the Deed, which includes the roles and responsibilities of both parties as far as privacy and security obligations.

### Privacy advantages for DDL users over the existing plastic driver licence

- The DDL is potentially more secure in that it is protected by device and JVO app security measures, including MFA as the app is set up on a device and password or PIN or biometric protection for each use.
- The DDL includes a range of other security features and further work is being undertaken to identify if other measures are needed.
- If an individual's device is lost or stolen, this does not mean the information is lost. A user can, with relative ease, add their DDL to another device.
- A customer's DDL can be verified in real-time. This means data can be instantly verified using by scanning the QR code displayed on the DDL within the JVO app.
- DDL users will have some choice about what information they display to verifier – the app will have three 'cards', which will display only relevant details, for example, the identity card will display the customer's photo, date of birth, and address, but not their driver licence details.

### 4.3 Residual privacy risk level

Overall, the DDL is likely to benefit individuals and it is being designed with privacy and trustworthiness as key considerations. Rather, the issues identified arise in the context of ensuring that privacy continues to be front of mind through the state-wide release and beyond.

In summary, with a number of important issues to manage both during and after state-wide rollout, IIS considers the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, continuous privacy coordination and monitoring arrangements, and close attention to and monitoring of the possible security risks for customers using a DDL.

## 5. FINDINGS AND RECOMMENDATIONS

# 5. Findings and recommendations

This section discusses relevant privacy risks and issues that IIS has identified during the PIA.

IIS has retained our analysis from the previous June 2023 PIA and added to the analysis any updated information that we have received from JVO and the DTP.

IIS made a total of 12 recommendation in our previous PIA. Since then, we note that JVO and the DTP have implemented a number of our recommendations. The status of implementation is displayed in each recommendation box. In key areas where we have included further recommendations, these are titled as Recommendation A, B, C and so forth.

IIS has not identified any areas of non-compliance with privacy or other legislation. The recommendations focus on ensuring privacy best practice.

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

## 5.1 IPP issues or risks

A high-level analysis of the DDL project against the IPPs is at [Appendix B](#). IIS considers that the DDL project is consistent with the IPPs. In particular:

- The project operates within the existing DTP's legal framework.
- The Deed authorises the JVO to collect, use and disclose personal information consistent with its roles in providing DDL infrastructure and the myVicRoads app.
- Anonymity is not practicable.
- The project will operate within Victorian borders.

The main IPPs where IIS has identified issues are in relation to transparency and openness, disclosure, security, access and correction, and privacy complaint handling.

### 5.1.1 Transparency – IPP 1 and IPP 5

Transparency provisions in the IPPs aim to allow individuals to make informed choices about providing information or using a service and to have a general understanding of how information about them is being handled. Transparency is both a matter of compliance as well as key to building public confidence and trust in the DDL.

The IPPs provide two transparency mechanisms:

- Specified details, usually a collection notice, provided at the point personal information is collected or as soon as possible thereafter (IPP 1.3).
- General information, usually via a privacy policy, about the type of personal information agencies collect and hold and how it is managed (IPP 5.1).

## 5. FINDINGS AND RECOMMENDATIONS

The Deed, at clause 39.6, mirrors these requirements and adds specific requirement to specify any law that requires collection of personal information by the State, or that personal information may be disclosed to the State. Clause 39.7 provides that collection notices must be provided to, or approved by, the Secretary [of DTP].

### 5.1.1.1 Privacy collection notice and privacy policy

In keeping with its policy and oversight roles for the DDL and the 'one licence, two channels' approach, the DTP will be seeking to ensure consistency in collection notices for the myVicRoads and Service Victoria apps. IIS was advised that the JVO has not yet finalised its collection statements. IIS understands that the JVO and Service Victoria will collaborate as the notices are finalised.

The IIS assessment drew on information provided, including terms and conditions (T&C) for myLearners, what we have seen of the JVO's approaches in other contexts (for example, viewing the VicRoads website) as well as DTP's feedback letter to JVO's terms and conditions and privacy materials.

We understand JVO's general approach to providing privacy information, including collection notices, for the state-wide release will be as follows:

- Provide link to the privacy policy on the VicRoads website.<sup>5</sup>
- For myVicRoads account, provide a link to the T&C which include a privacy statement – effectively a collection notice – and a link to the VicRoads privacy brochure.
- Registering for the DDL
  - Provide general advice, including FAQs, about the privacy and security features of the DDL, for example: 'with digital ID, you control what information you share, and who you share it with', 'having a digital driver licence in our myVicRoads app means your identity is kept safe using state-of-the-art security and privacy features', and the DDL is an 'easy, secure and private way' to access a licence. 'privacy and security of personal information is the highest priority in the digital driver licence's development'.<sup>6</sup>
  - Provide link to T&C at the point a customer logs into myVicRoads account to register for the DDL.
- When setting up the app, providing a link to T&C and the privacy brochure.
- Within the myVicRoads app, the Settings menu includes 'help and info' section, with links to T&C and privacy policy.
- Within the app, message on screen alerting customers to what QR code will show and verify if scanned, for example 'the person who scans this code will only verify your licence number [or 'your age/identity', or 'your age']. No other data will be shared'.<sup>7</sup>

---

<sup>5</sup> <https://www.vicroads.vic.gov.au/website-terms/privacy>

<sup>6</sup> <https://www.vicroads.vic.gov.au/licences/digital-driver-licence>

<sup>7</sup> MyVicRoads Digital Driver Licence Feature: QR Code, images on page 5.

## 5. FINDINGS AND RECOMMENDATIONS

IIS considers that this approach is likely to be consistent with the IPPs. It provides the necessary information and adopts a 'layered' approach, particularly with the short privacy messages below the QR code. IIS also agrees with the DTP's suggestion in its feedback letter to JVO's terms and conditions and privacy materials.

Additionally, we have identified some areas where additional action would contribute to good privacy practice.

- Privacy information is not prominent on the JVO website – a search is needed to find the privacy policy
- IIS notes that the JVO is currently updating the privacy policy to address the feedback from DTP. At the time of writing this report, IIS has not reviewed the draft privacy policy. One of the feedback items given was to include details regarding QR code scanning on the DDL. IIS is under the assumption that the updated privacy policy will contain a distinct section about DDL. We consider it good practice to include specific information about the JVO's role in managing R&L data, and about the DDL, in the policy, or provide links to comprehensive information elsewhere.

This might include:

- Collection and handling of information for identity verification
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential verifier handling a device
- How to report a device as lost or stolen to the JVO and/or to VicPol.
- The current information about the DDL on the website provides high-level assurances about privacy and security and some additional information. IIS notes that a Guide for Licence Checkers has been published to support licence checkers. However, there is still a lack of JVO comprehensive, detailed information about the operation of DDLs including the handling of personal information, security issues and protecting against risks, how the QR code works etc, on the website.
- While privacy information will be available once a customer enters the myVicRoads portal, there appear to be no privacy links or information (other than, as noted, high-level assurances) from the initial pages about the DDL.

IIS reviewed the collection notice currently available on Service Victoria's website which will be updated to reflect state-wide release (noting that it now currently only refers to the pilot).

IIS supports the clarity of the notice and did not find any issues under IPP 1.3. The notice uses plain English and gives a reasonably detailed overview of the Service Victoria DDL. IIS understands the JVO is aware of this notice and will take it into account in further work collection notices.

We make the following recommendations to address the issues identified.

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation A – Make privacy-related information about the DDL prominent and easily accessible

Make available comprehensive, plain English information about the operation of the DDL available in public web pages about the DDL. This should include information about the handling of personal information, security issues and protecting against risks, how the QR code works and so on.

**Who:** JVO and DTP

**Timeframe:** For state-wide release and ongoing

**Retained from previous PIA**

### Recommendation B – JVO's privacy policy to include or link to comprehensive DDL information

Include comprehensive DDL information for the full public rollout in the JVO's privacy policy, or in links from the privacy policy.

Include an additional 'extra privacy information' section in the policy or in relevant links on the information handling for DDLs, which should cover matters such as:

- Collection and handling of information for identity verification
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential verifier handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

**Who:** JVO and DTP

**Timeframe:** For state-wide release and ongoing

**Retained from previous PIA**

### Status of recommendations from previous PIA

IIS notes that the DTP, the JVO and Service Victoria have implemented the following transparency recommendations from the previous PIA.

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 1 – Project governance processes to ensure consistent, best practice privacy messages for both the myVicRoads and Service Victoria apps

Establish project governance arrangements that include processes to ensure that privacy messages delivered by the DTP, the JVO and Service Victoria are consistent, comprehensive and adopt best practices approaches. Make clear in the governance processes who is responsible for signing-off on privacy materials and monitoring their use.

**Who:** DTP, the JVO and Service Victoria

**Timeframe:** For full rollout and ongoing

**Status:** Implemented

### Recommendation 3 – Pilot collection notices to use plain English and be supported by an overview of the DDL

In developing privacy collection notices for the pilot, adopt a 'good practice' approach, consistent with Service Victoria's notice, which should include using engaging plain English and provide, in addition to the requirements of IPP 1.3, an overview of the JVO's DDL, including the information handling, the server retrieval process and the QR Code.

**Who:** JVO and DTP

**Timeframe:** For the external pilot

**Status:** Implemented

#### 5.1.1.2 Public communications and education

In addition to the specific requirements in the IPPs, active public awareness and education for DDL users and verifiers will support transparency about the project, and support individuals' ability to exercise their privacy rights and to use a DDL safely.

IIS is encouraged by the work DTP, JVO and Service Victoria have done to date in this area. In keeping with its role in ensuring the DDL experience, design, functionality and features will be same across both channels, the DTP is taking the lead on DDL communications and engagement.

## 5. FINDINGS AND RECOMMENDATIONS

The DTP, in collaboration with the JVO and Service Victoria, has developed a Communications and Engagement Plan (the C&E Plan).<sup>8</sup> The C&E Plan includes the narratives and key messages for the regional pilot as well as communications and engagements tactics and timings in preparation for the full rollout. The narratives and key messages provide a good high-level overview of the solutions offered by both Service Victoria and the JVO.

The Communications Team is also working on other collateral to promote public awareness and educations which includes factsheets, an instructional video for users as well as briefing packs. IIS considers these efforts to be important in not only driving uptake but also in ensuring that Victorians are adequately informed about the DDL and its processes.

IIS notes that the JVO has implemented some of the items in the C&E Plan, such as updating its webpage on the DDL to include FAQs, and publishing a Guide for Licence Checkers to support business awareness of DDLs and how they could use it in practice, including the steps to verify the licence, identity or age cards.

In addition, as part of the broader rollout of the DDL, IIS understands that the DTP and Service Victoria are planning to increase their engagement with businesses (that are licence checkers) in order to guide and support them. IIS supports this initiative and recommends for the DTP to continue its engagement with customers to better understand their pain points and needs but also as an opportunity to educate businesses about the licence verification process.

Additionally, IIS makes some further suggestions which would enhance the clarity and accuracy of privacy messages:

- The C&E Plan alludes to, but does not specifically make clear, some of the key differences between the two apps, in particular, what information is shared with verifiers. Customers are encouraged to adopt whichever app is best for them but it will be more difficult for them to make an informed choice if the differences are not clear.
- The JVO have included certain security advice for customers on the DDL webpage. In the interests of transparency and helping DDL customers to protect themselves, IIS encourages the DTP and the JVO to continue to update these as any threats emerge.
- The question of whether law enforcement bodies, or other verifiers, are able to request to hold a customer's device to view a DDL has been an issue in other jurisdictions. The C&E Plan does not currently provide advice on this for customers or verifiers. IIS understands that there will be no requirement for customers to hand over their devices. Although this has been made clear in the Guide for Licence Checkers, we consider this should also be made clear to all users (i.e. by including this in the FAQ).

---

<sup>8</sup> Communications and Engagement Plan (April 2023).

## 5. FINDINGS AND RECOMMENDATIONS

The above suggestions and those listed in Recommendation C below are based on best practice considerations. JVO and DTP should continue to bear them in mind as they develop and update the relevant communications materials.

The C&E Plan includes communications evaluation measures. For customers, the measure identified is an 'overall customer satisfaction score of >95%'. As previously mentioned, the JVO has not received any negative feedback since the pilot release, however there is no empirical measure of customer satisfaction yet. IIS understands surveys which includes a privacy satisfaction question have recently been sent out to users to obtain their feedback on the DDL.

As an ongoing practice, it is important for the JVO and Service Victoria develop a mechanism to continue to monitor customer feedback during the state-wide rollout. Customer feedback will assist the agencies in its continuous improvement work for the DDL.

Please also see [Section 5.3.2.2](#) where we discuss fraudulent use cases and the importance of communications as a control measure.

### Recommendation C – Ensure DDL communications, including privacy and security information, are accurate, consistent and fit-for-purpose

Ensure that communications for the DDL:

- Provide clear information about the differences between the JVO and the Service Victoria apps, in particular what information is shared with verifiers.
- Continue to monitor security risks and update the security advice as needed.
- Provide clear information to licence users that there is no requirement for them to hand over their devices to licence checkers, (i.e., include in the FAQs)
- Provide accurate advice about whether a plastic licence must be carried and the circumstances in which a plastic card might still need to be shown.

**Who:** JVO and DTP

**Timeframe:** For state-wide release and ongoing

**Retained from previous PIA**



## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation D – Continue to support engagement with businesses during state-wide release

Continue to support engagement with businesses to better understand their pain points and needs, as well as educating them about the licence verification process.

**Who:** DTP, JVO and Service Victoria

**Timeframe:** For state-wide release and ongoing

### Recommendation E – Continue to monitor customer feedback

Develop a mechanism to continue monitoring customer feedback (including on privacy matters) during the state-wide rollout.

**Who:** DTP, JVO and Service Victoria

**Timeframe:** For state-wide release and ongoing

### Status of recommendation from previous PIA

IIS notes that the following recommendation has been implemented.

### Recommendation 6 – Include privacy in pilot evaluation

Include privacy 'satisfaction' in the evaluation of pilot communications. Issues to consider could include understanding of the QR code content, whether customers had sufficient information to make an informed choice about using a DDL, and if they were confident that privacy and security would be protected.

**Who:** DTP

**Timeframe:** For the external pilot

**Status:** Implemented

### 5.1.2 Disclosure – IPP 2

IPP 2 states that personal information may only be disclosed for the primary purpose for which the information was collected. Under OVIC Guidance, it is considered a disclosure when others are allowed to view personal information even though it remains in the possession or control of its original collector. In this instance, we are discussing the scenario where licence information on the DDL is being disclosed to licence checkers which meets the primary purpose test of IPP 2.

## 5. FINDINGS AND RECOMMENDATIONS

During the period of preparing this PIA, IIS understands that there has been significant discussion between DDP, Service Victoria and JVO regarding the amount and kinds of information that should be disclosed. IIS notes that the JVO is strongly in favour of minimal information being displayed on the verifier side.

For the pilot, the JVO's disclosure of personal information for DDLs, other than displaying driver licence information to the customer, was very limited. The only personal information disclosed when a verifier scans the QR code or bar code for the driver licence view was (i) the licence number and (ii) the green tick and message that the licence is verified. Customers may also choose to allow a verifier to see, and take notes of, the information on their device. The approach taken by the JVO was different to Service Victoria's where more information is disclosed to licence verifiers depending on the specific use case (including the image of the licence holder).

IIS understands that the DTP has made a policy decision in regard to the above matter, taking into account trade-offs between usability and privacy. The DTP's position is a 'middle ground' between the Service Victoria and JVO positions. The kinds of information that will be displayed on the verifier's app, upon scanning the customer's DDL QR Code, are the following:

- Verification of licence – photo, first and last name, licence status, proficiency.
- Verification of age – indication of whether the customer is over 18 (green tick for yes, red cross for no), photo.
- Verification of identity – photo, first and last name, address.

IIS notes that minimal information is involved in the verification of age, which is privacy positive. This would occur in the context of entering pubs and clubs, and which would pose a heightened privacy risk to patrons if more of the person's information was to be revealed (e.g., to an unscrupulous bouncer).

IIS understands that the inclusion of the photo as part of the information being displayed to verifiers is a mitigation against spoofing of the DDL (i.e., where a person alters the appearance of the credential on a jailbroken phone). In such scenarios, the verification process may return a correct verified status even though the DDL has been tampered with; the correct customer photo that is displayed to the verifier would enable them to identify that the person has changed the photo on their side.

Overall, IIS considers that the information proposed to be disclosed on the verifier side is appropriately limited to the verification use case and that the DTP has achieved a good balance between usability and privacy.

Additionally, as part of our discussion with the DTP, JVO and Service Victoria, it was acknowledged that there continues to be a need for certain businesses to retain some or all licence information as part of their legislative or operational requirements.

## 5. FINDINGS AND RECOMMENDATIONS

We note that certain matters such as policy decisions, privacy decisions, and product design will require further consideration to address these requirements in the context of the DDL. It is beyond the scope of this PIA to assess these issues. However, IIS cautions against conflating the time-limited sharing of personal information for DDL verification purposes with the broader sharing (and subsequent collection) of such information for business retention purposes.

### 5.1.3 Security – IPP 4

IPP 4 requires agencies to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. The DTP and the JVO are also subject to the VPDSF and VPDSS. The VPDSS prescribes a minimum set of mandatory requirements across all security areas including governance, information, personnel, ICT and physical security. The VPDSF provides direction to Victorian public sector agencies or bodies, or in the case of the JVO, brought in under s 84(3) of the PDPA, on their data security obligations.

As noted in the PIA scope ([Section 2.1](#)) the PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features.

Business Impact Levels (BIL) are used to determine the security value of public sector information. BILs describe the potential harm or damage to government operations, organisations or individuals if there were a compromise to the confidentiality, integrity or availability of public sector information. The DTP has undertaken an Information Value Assessment (IVA) 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Factors taken into account include that:

- The DTP is sharing images and R&L data together, which it would usually only do in limited circumstances because of the sensitivity and high value of the data
- The potential volume of data to be shared with the JVO and Service Victoria
- The impact on public confidence and community safety if the integrity of drivers licence is impacted.

IIS has not validated this assessment as part of the PIA, but has not noted any issues.

#### 5.1.3.1 System security

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

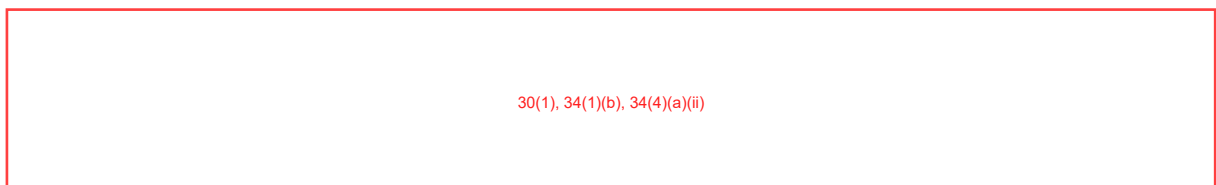
The JVO has noted a number of design features for the project that aim to mitigate the risks. It has also taken steps, including as required under the Deed, to manage its security approaches. The IVA and the protected designation require rigorous assessment of systems and processes to determine what more is needed. IIS understands that the JVO has addressed the security recommendations in the first Service Victoria DDL PIA.

Security actions that are relevant for this PIA include:

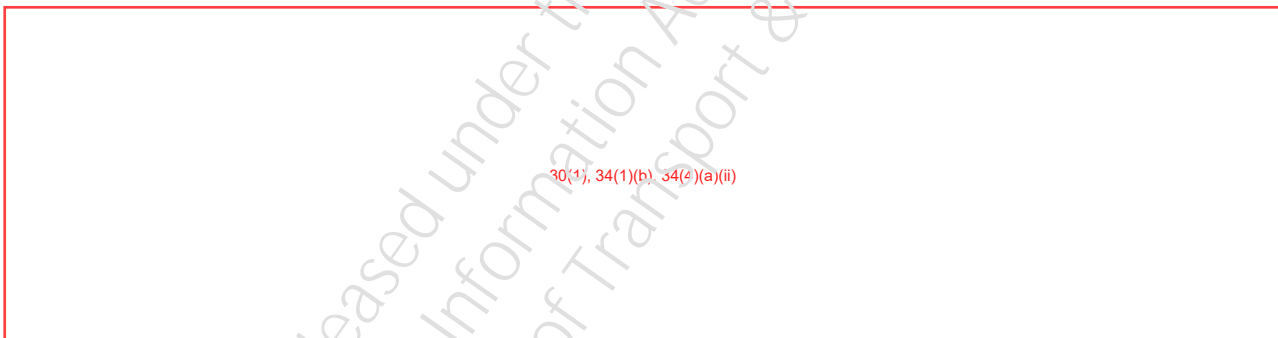
- **Incorporation of Security by Design in the development of the DDL**
  - The DDL has been designed with privacy and security recommendations from ISO 18013-5 in mind. The recommendations include: minimising data wherever possible; embedding privacy in design, flows, and architecture; keeping operations visible and transparent to the customer; designing for user-centricity and user control.



- **Security assessments**



## 5. FINDINGS AND RECOMMENDATIONS



Although IIS has not done a security assessment, we consider the security approach for the myVicRoads is likely to limit both privacy and security risks. We have not identified any issues of concern.

### Status of recommendation from previous PIA

#### Recommendation 7 – Record DDL related privacy risks on the project risk register

Include privacy risks to individuals using a DDL in the risk register and ensure that these risks are continuously monitored.

**Who:** JVO

**Timeframe:** Before full roll out

**Status:** Implemented

## 5. FINDINGS AND RECOMMENDATIONS

### 5.1.3.2 Security for DDL customers

25

IIS agrees that a number of features of the JVO DDL appear to offer security advantages, possibly more than a plastic licence. These include:

- A DDL will quickly fail to display if the DTP has been notified that a licence has been lost or stolen.
- MFA is mandatory as part of setting up a DDL on a device, and when re-logging into a myVicRoads account.
- Data is updated regularly, meaning changes of address or licence conditions are easily refreshed.
- Customers can delete the DDL from their device.
- The inclusion of a card number on licences, which can be easily replicated on either the myVicRoads or Service Victoria app, depending on which is being used provides an additional element to protect identity in the event of a data breach.

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(i)

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

Overall, IIS has not identified any significant areas of concern from a privacy perspective with the JVO's security approach for the DDL. The approach seems consistent with privacy and security by design and is positive and comprehensive. IIS understands that the JVO and DTP have implemented our security recommendations, noting that at the time of writing the DTP and JVO are actively considering options for limiting address display. We make no further recommendations.

## 5. FINDINGS AND RECOMMENDATIONS

### Status of recommendations from previous PIA

#### Recommendation 8 – Continue to assess security risks for individuals and provide up-to-date information on risks and mitigations

Continue to assess and monitor risks of identity fraud or other misuse of DDL that might pose risks to individuals.

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Provide up to date information for customers on possible security risks and how to mitigate them.

**Who:** JVO

**Timeframe:** For the full rollout and ongoing

**Status:** Implemented

#### Recommendation 9 – Explore options for limiting address display on the DDL driver licence view

Explore options for allowing differential display of address on the driver licence view.

**Who:** DTP and JVO

**Timeframe:** For the full roll out

**Status:** Implemented



## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 10 – Clarify requirements for the handling of individuals' devices for DDL validation

Clarify whether validators may take an individual's device when checking a DDL, including if necessary, by considering legislative change.

**Who:** DTP

**Timeframe:** For the full roll out

**Status:** Implemented

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

### 5.1.4 Access and correction – IPP 6, and privacy complaint handling

IIS notes that the JVO and the DTP have some shared responsibilities in the handling of customer enquiries and complaints including privacy complaints. These are subject to the Deed and to processes and workflows developed. IIS understands these would also address any requests for access to or correction of personal information. The DTP will remain the responsible for requests relating to R&L data but there may be cases for the JVO or where there is a shared responsibility.

The JVO customer channels should guide customers to the appropriate source of help. However, given that Service Victoria is also offering DDLs there is a (possibly low) risk that customers will approach the wrong organisation to seek help or make a complaint. IIS encourages the organisations to ensure, via governance arrangements, that there are arrangements in place to ensure that there is ‘no wrong door’ and customers are directed and assisted to the right place.

Additionally, IIS understands that there are existing escalation processes in place for JVO to engage with the DTP’s Vulnerable Customers Team when interacting with customers who are facing (1), 34(1)(b), 34(4)(a)

30(1), 34(1)(b), 34(4)(a)(ii)

IIS was told that these processes will also be applied in relation to any (1), 34(1)(b), 34(4)

30(1), 34(1)(b), 34(4)(a)(ii)

with the DDL. The DTP Vulnerable Customer’s Team assist clients that are affected by family violence with their registration and licensing requirements, which includes changing number plate and licences due to family violence. We recommend for the JVO to monitor the effectiveness of these processes, to ensure that (1), 34(1)(b), 34(4)(a)(ii)

continue to receive the appropriate support and assistance, including in the context of the DDL.

#### Recommendation F – Monitor the effectiveness of the processes when engaging the DTP Vulnerable Customers Team

Monitor the effectiveness of the processes when engaging the DTP Vulnerable Customers Team, to ensure that (1), 34(1)(b), 34(4)(a)(ii) receive the appropriate support and assistance when faced with issues relating to the DDL.

**Who:** JVO

**Timeframe:** Ongoing

## 5.2 Governance

### 5.2.1 Project governance

The DDL Project is now moving to its state-wide implementation phase. IIS has been impressed with the emphasis to date on both privacy and security by design in the design and built phases of the DDL. Strong privacy and security protective measures have been included. IIS understands that for the as long as the project is under ‘Delivery’ mode, project governance including in relation to privacy will be led by the Steering Committee.

## 5. FINDINGS AND RECOMMENDATIONS

Additionally, IIS notes that the Deed requires the JVO to have a privacy management plan. It is outside the scope of the PIA to comment on the JVO's privacy management more generally. However, IIS considers the privacy management plan could help ensure a coordinated best practice approach and for privacy to remain a priority in implementation, evaluation, and monitoring phases of the DDL. We are under the assumption that the JVO's privacy management plan will dictate the governance arrangements post 'Delivery' mode.

At the time of writing the report, IIS did not review the privacy management plan as we were advised that the plan was still being finalised. For that matter, we have retained the relevant recommendation.

### Recommendation G – Strengthen DDL privacy governance arrangements including by relevant provisions in the JVO privacy management plan

Identify or establish a process that will allow coordination and monitoring of privacy approaches relevant to the DTP, the JVO and Service Victoria. Ensure these processes are effective so that there is 'no wrong door' for requests for access and correct, or for lodging privacy complaints.

In completing the JVO privacy management plan, include strategies to ensure a coordinated best practice approach, and to ensure that privacy remains a priority in implementation, evaluation, and monitoring phases of the DDL.

**Who:** JVO

**Timeframe:** For post 'Delivery' mode

**Retained from previous FIA**

### 5.2.2 Privacy by Design and future developments

PbD has been a feature of the DDL project development to date. In part, this has been driven by the JVO's customer first focus, recent data breaches and ISO and other international standards. In stakeholder consultations, the JVO demonstrated that privacy remain key consideration of DDL design and development.

IIS encourages the JVO to continue this approach, which will clearly remain relevant as the DDL is implemented and as further enhancements are introduced. IIS understands these might include:

30(1), 34(1)(b), 34(4)(a)(ii)

- DDLs available for learners and probationary permits

## 5. FINDINGS AND RECOMMENDATIONS

- Displaying the number of demerit points a person has accrued (preferably this would be displayed 'below the fold')
- Alerts or notifications that a learner permit and/or driver licence is due to expire, or that a future ban is about to commence.

IIS also notes that the JVO is committed to ensure that PIAs are conducted at relevant points in the development process. As such, we are satisfied that the JVO has implemented Recommendation 12 from the previous PIA.

### Status of recommendation from previous PIA

#### Recommendation 12 – Take steps to ensure continued PbD approach in the DDL's further development

Continue the current PbD approach for the DDL, including by conducting further PIAs before making changes to the DDL, for example sharing licence information with validators, or introducing notifications, or display of status or demerit points, which could impact on individuals' privacy.

Ensure privacy management processes, such as the privacy management plan, or other project management or governance processes, are in place to ensure the PbD approach continues to be strong feature of the JVO DDL.

**Who:** JVO

**Timeframe:** For full rollout and ongoing

**Status:** Implemented

### 5.3 Additional considerations – negative use cases

The assessment of privacy risks and identity theft/fraud risks have been specifically considered in this PIA by reference to use cases concerning 30(1), 34(1)(b), 34(4)(a)(ii) and fraud.

#### 5.3.1

30(1), 34(1)(b), 34(4)(a)(ii)

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

30(1), 34(1)(b), 34(4)(a)(i)

## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(ii)

### 5.3.2 Fraudulent use cases

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4) a)(ii)

On balance, the risks of fraudulent activity exist for both the DDL and physical licence cards. Overall, IIS considers the potential for misuse by bad actors to create a false DDL credential is mitigated to a significant extent by the DDL controls including for example, real time verification and the capacity to respond quickly to identified security issues. These are real advantages compared to the status quo of physical cards, which have their own risks with fraudulent use cases.

---

<sup>9</sup> <https://www.vicroads.vic.gov.au/licences/digital-driver-licence/verify#:~:text=need%20further%20verification,-.The%20most%20secure%20way%20to%20check%20a%20digital%20driver%20licence.one%20the%20customer%20is%20using.>



## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(ii)

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

6. APPENDIX A – METHODOLOGY

## 6. Appendix A – Methodology

### 6.1 PIA approach

IIS took the following steps to carry out the PIA:

- *Planning* with the DTP and JVO to confirm the approach, scope and deliverables of the PIA
- *Gathering information* by reading documents and meeting with personnel from the DTP and the JVO
- *Analysing the information* against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy good practice
- *Identifying privacy risks* and developing ways to mitigate those risks
- *Drafting the PIA report* – in this case, updating the June 2023 PIA report in relevant places, and providing this to the DTP and JVO for comment
- *Finalising the PIA report* following feedback from the DTP and JVO.

### 6.2 Documents reviewed

Documents reviewed	
<b>DTP documents</b>	
1.	Communications and Engagement Plan April 2023
2.	Concession Deed, privacy and <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>
3.	<span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>
4.	<span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>
5.	Department of Transport & Planning, Information Value Assessment
6.	<u>DTP Privacy Policy</u>
7.	DTP Risk Matrix
8.	Establishing an identity with VicRoads
9.	Separation model, JVO and State
10.	Victorian Government Gazette, No. S 523, October 2022, application of PDPA to JVO
11.	<span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>

6. APPENDIX A – METHODOLOGY

Documents reviewed	
12.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
13.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
<b>The JVO documents</b>	
1.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
2.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
3.	myLearners T&C
4.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
5.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
6.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
7.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
8.	MyVicRoads T&C for use <a href="https://www.vicroads.vic.gov.au/website-terms/individual-terms-and-conditions">https://www.vicroads.vic.gov.au/website-terms/individual-terms-and-conditions</a>
9.	Privacy policy at <a href="https://www.vicroads.vic.gov.au/website-terms/privacy">https://www.vicroads.vic.gov.au/website-terms/privacy</a>
10.	Protecting Your Privacy Brochure (available from myVicRoads website, including by search or link in T&C)
11.	Rough scope of high-level assessment
12.	Service Victoria draft privacy collection notice (from May 2022 PIA)
13.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
14.	Response from JVO re privacy conditions, Oct23
15.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
16.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
17.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
18.	Signed letter to JVO - DDL TCs and privacy materials
19.	Use cases DDL for IIS (revised with Service Victoria comments)

## 6. APPENDIX A – METHODOLOGY

Documents reviewed	
<b>Relevant Service Victoria documents</b>	
1.	Draft Service Victoria Privacy Collection Notice for DDL pilot (May 2022)
2.	<div style="border: 1px solid red; padding: 5px; text-align: center;">30(1), 34(1)(b), 34(4)(a)(ii)</div>
3.	Service Victoria DDL FAQs <a href="https://service.vic.gov.au/early-access/digital-driver-licence/home">https://service.vic.gov.au/early-access/digital-driver-licence/home</a>

### 6.3 Meetings held

Meetings held	Date
Pre kick-off meeting: <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• the DTP personnel</li> </ul>	10 October 2023
Kick-off meeting with the JVO <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• the JVO personnel</li> </ul>	18 October 2023
PIA information gathering meeting – <div style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</div> <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• DTP personnel</li> <li>• JVO personnel</li> </ul>	23 October 2023
PIA information gathering meeting – <div style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</div> <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• JVO personnel</li> </ul>	25 October 2023
PIA information gathering meeting – <div style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</div> (DTP) <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• DTP personnel</li> </ul>	31 October 2023

## 7. Appendix B – Assessment against the IPPs

The following table sets out IIS's high-level assessment JVO DDL against the IPPs in the context of the expected state-wide full release in December 2023. This PIA focuses on the information flows for the myVicRoads app as described at [Section 3.5.3](#). The information flows between DTP, JVO and Service Victoria will be assessed in a separate PIA.

In making our assessment, we note that:

- The JVO app will display very limited health information in the form of licence codes. This would be subject to the HPPs in the HRA. IIS notes that the HPPs cover similar issues to the IPPs and for this PIA has not undertaken a separate assessment.
- The JVO is handling R&L data on behalf of the DTP, which retains ownership of the data. The DTP continues to be responsible under privacy laws for the data. The JVO has specific privacy obligations under the Deed and separately is also directly subject to privacy laws.
- The JVO DDL approach (where data is displayed but not stored on an individual's device, and is not shared with verifiers (other than for law enforcement verification where driver licence number is contained in the bar code)) involves limited direct disclosure of personal information. However, the process would generally involve the individual in showing the DDL on their device to a verifier. There is also a small, but not impossible, chance that data would be inadvertently disclosed if the device is subject to fraudulent misuse.

IIS also notes that where our assessment has not identified specific issues for this PIA, that is not meant to indicate there is no privacy work to be done. IIS anticipates that usual privacy compliance and monitoring would occur.

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 1 – Collection</b></p> <p>An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation’s Privacy Policy.</p>	<p>The DDL involves a re-use of existing information the DTP holds, not a new collection for DTP.</p> <p>Under the Deed, the JVO will be collecting and handling some personal information on behalf of the DTP.</p> <p>The introduction of DDL is a new way of providing driver licences – and as such both the JVO’s privacy policy and collection notice is being updated. The Deed states the Secretary must approve JVO collection notices and privacy policy. We also understand that the DTP policy intent is that the privacy information for the myVicRoads and Service Victoria apps will be consistent.</p> <p>See discussion at <a href="#">Section 5.1.1</a>.</p>
<p><b>IPP 2 – Use and disclosure</b></p> <p>Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual’s consent, for a law enforcement purpose, or to protect the safety of an individual or the public.</p>	<p>The DTP and JVO’s use of R&amp;L data for DDLs licence is consistent with the purpose of collection.</p> <p>Privacy law obligations, as well as the Deed, ensure that JVO must only use or disclose personal information as permitted under the Deed.</p> <p>In general, as noted above, the JVO is taking a cautious approach to disclosures of personal information for the myVicRoads app. <span style="border: 1px solid red; padding: 2px;">1), 34(1)(b), 34(4)(a)</span></p> <div style="border: 1px solid red; padding: 10px; text-align: center; margin: 10px 0;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div> <p>See additional discussion of disclosure in the context of QR code verification at <a href="#">Section 5.1.2</a>.</p> <p>Overall, IIS considers that the information proposed to be disclosed on the verifier side is appropriately limited to the verification use case and that the DTP has achieved a good balance between usability and privacy.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 3 – Data quality</b></p> <p>Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.</p>	<p>The DDL should not diminish and may enhance data accuracy of driver licence information.</p> <p>Changes to driver licence details or status will be subject to pilots and roll-out and will be reflected in the DDL quickly.</p> <p>The DTP's requirements and JVO's design are such that the myVicRoads app does not collect or hold identified personal information. The one source of truth of driver licence information remains with the DTP.</p> <p style="border: 1px solid red; padding: 2px; display: inline-block;">30(1), 34(1)(b), 34(4)(a)(ii)</p> <p style="border: 1px solid red; padding: 2px; display: inline-block;">30(1), 34(1)(b), 34(4)(a)(ii)</p> <p>No issues identified.</p>
<p><b>IPP 4 – Data security</b></p> <p>Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.</p>	<p>The DTP and JVO have in place detailed security management processes and have commenced or undertaken detailed security risk assessments for the DDL.</p> <p>At this point, there are some issues to work through. See further discussion at <a href="#">Section 5.1.3</a>.</p>
<p><b>IPP 5 – Openness</b></p> <p>Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation's Privacy Policy.</p>	<p>Both the DTP and the JVO have in place or will be updating or developing privacy policies, privacy notices and other privacy information. The intention is that the materials will be consistent and that individuals are easily able find relevant information to inform their decisions. IIS also considers that best practice would be to support more formal material with engaging, plain English information about DDLs and possible risks or issues.</p> <p>See further discussion regarding transparency and public communications at <a href="#">Section 5.1.1</a>.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 6 – Access and correction</b></p> <p>Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982 (Vic).</p>	<p>The introduction of the DDL should not affect current processes for access and correction. However, JVO Service Victoria and the DTP should ensure respective responsibilities are clear and that processes are built with a ‘no wrong door’ approach.</p> <p>See further discussion at <a href="#">Section 5.1.4</a>.</p>
<p><b>IPP 7 – Unique identifiers</b></p> <p>A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.</p>	<p>Driver Licence numbers are unique identifiers in terms of the PDPA.</p> <p>Driver licence numbers will appear on the DDL. However, the DDL project does not involve the assignment of new unique identifiers.</p> <p>No issues identified.</p>
<p><b>IPP 8 – Anonymity</b></p> <p>Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.</p>	<p>Not relevant for the DDL – identification is a required part of acquiring or using a DDL.</p>
<p><b>IPP 9 – Transborder data flows</b></p> <p>If an individual’s personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.</p>	<p>As far as IIS understands, the DDL processes are contained within Victoria.</p> <p>No issues identified.</p>



7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for DTP and JVO
<p><b>IPP 10 – Sensitive information</b></p> <p>The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.</p>	<p>Driver licence processes do not involve the collection of sensitive information as defined, but do involve some biometric and health information (See <a href="#">Section 3.6.2</a>). Such information is part of the R&amp;L data that the DTP has already collected.</p> <p>No issues identified.</p>

Released under the Freedom of Information Act 1982  
 Dept of Transport & Planning

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

INFORMATION INTEGRITY SOLUTIONS PTY LTD

PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438

F: +61 2 9319 5754

E: [contact@iispartners.com](mailto:contact@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

ABN 78 107 611 898

ACN 107 611 898



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

**Report: 15 June 2022**

**Department of Transport, Victoria**

**Sensitive**

# PRIVACY IMPACT ASSESSMENT - DIGITAL DRIVER LICENCE PROJECT



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

## Contents

Glossary	1
1. Executive summary	2
1.1 IIS's overall view	3
1.2 Recommendations	4
2. Introduction	6
2.1 PIA scope	6
2.2 About this report	6
3. Project description	8
3.1 Background	8
3.2 Project objectives and scope	8
3.2.1 Objectives and expected benefits of the project	8
3.3 Project status	9
3.4 About the DDL	9
3.5 Participants in the DDL Project MVP	10
3.5.1 The DoT	10
3.5.2 Service Victoria	11
3.5.3 Checkers – Victoria Police	11
3.5.4 Checkers – other, including pubs and clubs	11
3.5.5 Victorian citizens using a DDL	12
3.6 Nature of systems and information flows	12
3.6.1 Key system components	12
3.6.2 Kinds of information involved	13
3.6.3 Overview of information flows	14
3.7 Legal framework	18
3.7.1 Victorian laws	18
3.8 Project governance	20
4. Approach to risk analysis	21
4.1 Inherent privacy risks	21
4.2 Positive privacy aspects	22
4.3 Residual privacy risk level	23
5. Findings and recommendations	24
5.1 IPP issues or risks	24
5.1.1 Transparency – IPP 1 and IPP 5	24

## CONTENTS

5.1.2	Security – IPP 4	28
5.1.3	Access and correction – IPP 6, and privacy complaint handling	32
5.2	<b>Governance</b>	<b>33</b>
5.2.1	Project governance	33
5.2.2	Privacy by Design (PbD) and future developments	33
6.	<b>Appendix A – Methodology</b>	<b>35</b>
6.1	PIA approach	35
6.2	Documents reviewed	35
6.3	Meetings held	36
7.	<b>Appendix B – Assessment against the IPPs</b>	<b>39</b>

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## Glossary

Abbreviation or term	Expansion or definition
(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
34(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
IIS	IIS Partners
IPA	Information Protection Agreement
IPP	Information Privacy Principle
JV Partner	The DoT's Joint Venture Partner, still to be selected
JWT	Javascript Web Token
LOA	Level of Assurance
MVP	Minimum Viable Product
OVIC	Office of the Victorian Information Commissioner
PDPA	<i>Privacy and Data Protection Act 2014</i>
PIA	Privacy Impact Assessment
QR Code	Quick Response Code
R&L	Registration & Licensing
The DoT	Department of Transport
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VicPol	Victoria Police

## 1. EXECUTIVE SUMMARY

### 1. Executive summary

The Department of Transport (the DoT) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents; the DDL will be made available through the Service Victoria platform. A DDL will allow a licence holder to access an electronic version of their licence on a mobile device and present it in place of the physical licence for two primary use cases.

The first phase of the DDL Project is to produce a Minimum Viable Product (MVP), which will be tested via an internal and external pilot. The MVP would be a replication of the data and attributes from the existing Victorian driver licence to a digital credential through the Service Victoria digital wallet, with two primary use cases:

- Entitlement to drive
- Casual proof of age and photo.

The DoT will share its driver licence data with Service Victoria in order to deliver this product. Service Victoria is responsible for the design and release of the DDL. Due to the quantity and sensitivity of personal information that will be shared with and used by Service Victoria, the privacy impacts of the DDL Project need to be carefully examined. The DoT has engaged IIS Partners (IIS) to conduct a Privacy Impact Assessment (PIA) on the first phase of the DDL Project. The scope of the PIA covers privacy risks associated with:

- Data flows between the DoT and Service Victoria
- Security of the information
- Onboarding and user experience in the Service Victoria digital wallet
- Features and use cases within the MVP project scope
- Core privacy requirements under the Information Privacy Principles (IPPs).

In undertaking this PIA, IIS considered:

- Privacy principles in Victorian privacy law,
- Relevant legislation such as *Road Safety Act 1986* and the *Service Victoria Act 2018*
- Guidance materials published by the Office of the Victorian Information Commissioner and the Office of the Australian Information Commissioner
- Privacy good practice stemming from IIS's knowledge and experience.

This report:

- Provides background to the project, including key project participants and roles, key systems and information flows, and the relevant legal framework.



## 1. EXECUTIVE SUMMARY

- Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

The PIA methodology is included in the Appendices.

### 1.1 IIS's overall view

30(1), 34(1)(b), 34(4)(a)(ii)

- The project will involve the transfer of R&L data – which is considered very valuable and sensitive – from the DoT to Service Victoria to display DDLs.
- The DoT will be combining and transferring driver images as well as R&L details. The DoT considers that this adds to the project risks. IIS agrees this is a risk to the extent that it could be compromised (even if very unlikely)
- The project is in its initial phases Service Victoria has undertaken considerable consultation and design work in collaboration with the DoT. The DDL future directions are now subject to formal agreement and approval on matters including final design, security and governance, and on the outcome of two planned pilots.

30(1), 34(1)(b), 34(4)(a)(ii)

- The DoT is seeking further information from Service Victoria so that it can assess its security approaches and risk management in the context of the DDL.
- Service Victoria's design has taken account of possible security risks for DDL users. However, DoT is currently conducting further security assessment processes. IIS notes these would be concluded before the project proceeds for the external pilot.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including how checkers can interact with their devices, or handle personal information displayed via the DDL – can have a significant impact on them and jeopardise uptake of the solution.

IIS has not identified any show-stopping privacy issues for the project. Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. Taking into account the positive privacy aspects such as the emphasis on data minimisation, the avoidance of a new digital footprint, the DDL security features, and expected detailed governance arrangements, we consider that the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to the decisions made about security levels, governance, etc. and to systems being in place.



## 1. EXECUTIVE SUMMARY

IIS has identified the following key privacy risks and issues for consideration at this point in the project:

- **Transparency and privacy complaint handling**
  - Public communications are planned but are yet to be developed – they will need to address a range of issues to ensure the risks as well as positives of using a DDL are known
- **Security**
  - There are important security issues, including in relation to identity verification, data classification and security approaches, to resolved before the pilots and full roll out of a DDL – privacy and workability for DDL users need to be considered
  - If not already, privacy risks for individuals should be included in project privacy risk registers and monitored.
- **Privacy governance**
  - As more detailed arrangements for ongoing project governance are settled, they need to ensure there are clear privacy roles and responsibilities, including for monitoring privacy outcomes
  - There are future product decisions yet to be made, these should be made with privacy by design in mind.
  - Continuing the use of privacy by design will be important as the DDL project proceeds.

### 1.2 Recommendations

Our risk analysis acknowledges that the DDL project, although well advanced in product development, is in its early stages in other respects. For each recommendation, we have suggested who would be responsible for carrying out the recommendation (the DoT, Service Victoria, or both) and the timeframe for completion. We have identified some issues that should be addressed for the external pilot. However, most issues should be resolved before the full launch of the DDL, or are matters that require ongoing attention.

Recommendations	Who	Timeframe
<b>Recommendation 1</b> – Ensure that project agreements and governance arrangements provide for a process for ensuring that privacy messages are consistent and adopt best privacy practice	Service Victoria & DoT	For MVP and ongoing
<b>Recommendation 2</b> – Service Victoria and DoT privacy policies to include comprehensive DDL information	Service Victoria & DoT	For MVP and ongoing

1. EXECUTIVE SUMMARY

Recommendations	Who	Timeframe
<b>Recommendation 3</b> – Public communications should provide comprehensive privacy and security information	Service Victoria & DoT	For MVP and ongoing
<b>Recommendation 4</b> – Ensure decisions on security posture are made before the external pilot and are reflected in DDL customer information	Service Victoria & DoT	For MVP and Ongoing
<b>Recommendation 5</b> – Record DDL related privacy risks on risk register	Service Victoria & DoT	Before the DDL design and go-live decisions are finalised
<b>Recommendation 6</b> – Clarify and communicate requirements for the handling of individuals devices for DDL checking	Service Victoria & DoT	For MVP and ongoing
<b>Recommendation 7</b> – Ensure project governance arrangements include clear privacy roles and responsibilities, including for monitoring privacy outcomes	Service Victoria & DoT	For MVP and ongoing
<b>Recommendation 8</b> – Continue to adopt privacy by design in the DDL's further development	Service Victoria & DoT	Ongoing

## 2. Introduction

The DoT and Service Victoria are working to bring digital driver licences to Victorian residents, to be made available through the Service Victoria platform. The DoT engaged IIS to conduct a PIA on the first phase of the DDL project (the project) in Victoria. The project is being developed in the context of the VicRoads Modernisation Program, and the selection of a Joint Venture (JV) partner to deliver some functions.

### 2.1 PIA scope

Service Victoria is responsible for the design of the DDL, in accordance with the DoT's specified standards. DoT is also the data owner and will provide the data to populate the DDL. The PIA will entail end-to-end consideration of privacy issues that could have an operational impact from the perspective of both the DoT and Service Victoria.

The first phase of the project is the development of a Minimum Viable Product (MVP), which comprises an internal test pilot and a regional external pilot. The purpose of this PIA is to identify any privacy issues that might arise from the project's design and initial implementation approaches, and to make recommendations to address the potential issues.

In providing this report, IIS makes the following qualifications.

- The PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features
- The PIA is based on information gathered from, and provided by, the DoT and Service Victoria
- IIS does not provide legal advice; rather we provide strategic privacy and cyber security advice.

### 2.2 About this report

The report is structured to provide an overview of the DDL project, explain IIS's approach to risk analysis, analyse privacy issues according to the project scope, and provide additional context to the PIA work:

- **Project description** ([Section 3](#))  
Provides background to the DDL Project, key project participants and roles, key systems and information flows, and the relevant legal framework.
- **Approach to risk analysis** ([Section 4](#))  
Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.

## 2. INTRODUCTION

- **Findings and recommendations** ([Section 5](#))

Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

- **Appendix A – Methodology** ([Section 6](#))

Summarises our methodology, including list of documents reviewed and meetings held.

- **Appendix B – High-level assessment against the IPPs** ([Section 7](#))

Provides a high-level assessment of the DDL project against the IPPs and notes risks areas, which are discussed in detail in [Section 5](#).

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## 3. PROJECT DESCRIPTION

### 3. Project description

#### 3.1 Background

Service Victoria and the DoT are working to bring DDLs to Victorian residents. Three out of six Australian state and territory jurisdictions have either trialled or have a legislation-based DDL. Service Victoria has identified that there are 4.6 million active Victorian customers who use the Service Victoria mobile application, and over 4 million Victorians possess a driver licence. Service Victoria has been progressing delivery of the DDL in collaboration with the DoT.

The DDL will replicate data and attributes from an existing plastic Victorian driver licence to a digital credential. The DDL will have two primary use cases:

- Entitlement to drive whilst on the road
- Casual proof of age and photo for licenced venues and businesses such as supermarkets, convenient stores, tobacco retailers, etc.

The project is currently working towards an MVP, which will be tested via internal and external pilots. At the MVP stage, the DDL will be supplementary to the physical driver licence and will not replace it. The existing laws requiring drivers to carry a physical driver licence will remain enforceable.

#### 3.2 Project objectives and scope

##### 3.2.1 Objectives and expected benefits of the project

The DDL is consistent with the Victorian Government's digital strategy, which is expected to deliver cost savings, and better, fairer, and more accessible services, and a digital ready economy.

The expected benefits of the DDL for Victorian drivers are:<sup>1</sup>

- Freedom – After the pilots, most customers (except those from a cohort to which compulsory carriage requirements apply) will be able to leave their physical wallet at home.
- Peace of mind – The customers know their DDL is always on their phone as a backup.
- Convenience – 89% of the consulted customers indicated that they believe the DDL to be more convenient than a physical driver licence because they always carry their phone with them.
- Security – Customer's personal information is protected and only accessible via user login, or 6-digit PIN.
- Privacy – Information sharing can only be initiated by the customer, and the intention is that where circumstances permit, customers will be able to limit the amount of information exchanged.
- Up-to-date data management – Customers using a DDL have access to real time up to date information about the status of their licence; whether it is valid or has expired or has been suspended.

---

<sup>1</sup> See the 050522.DDL.Pilot.Scope.UC.Roadmap.

### 3. PROJECT DESCRIPTION

#### 3.3 Project status

Service Victoria and the DoT are taking an iterative approach to the DDL project. While Service Victoria and the DoT have undertaken considerable development work, the project is still in its early stages, particularly as far as security assessments and technical integration work required to consume driver licence data. There are also other elements, including the extent of JV partner involvement, governance, operational support and service level agreements, still to be finalised.

The MVP process will include two pilots:

- Internal pilot, which will test the DDL end-to-end journey, including identity verification, adding the DDL to the Service Victoria's Digital Wallet and the communication between Service Victoria and the DoT systems. This is only for full-licence car drivers, and without the QR Code. The DoT will not transfer 'real' data to Service Victoria for this pilot.
- Regional external pilot, which may take place in Ballarat with a focus on motorcycle, heavy and light vehicles for full licences holders above 21 years old. The external pilot will test matters including the use of the QR code verification by local business and authorities such as Victoria Police (VicPol). As noted, at the MVP stage, drivers will still need to carry their plastic licence.

The first phase of the internal pilot was successfully deployed commencing with internal rollout to Service Victoria on 18<sup>th</sup> May 22. The project is leveraging with an agile (phased) approach having agency onboarding in intervals. DoT have been invited to the pilot phase and the projection is to have DoT onboarded from 14<sup>th</sup> – 17<sup>th</sup> June before proceeding the next agency group.

The outcomes from the pilots will inform further development of the DDL. The further phases of the project are not fully determined at this stage and are out of scope for this PIA. They are expected to include a full public launch with all licence types and potential real-time data, and iterations with customer feedback. Future use cases are also currently in consideration, such as including push notifications (e.g., licence renewal, demerit points notification, change in licence status).

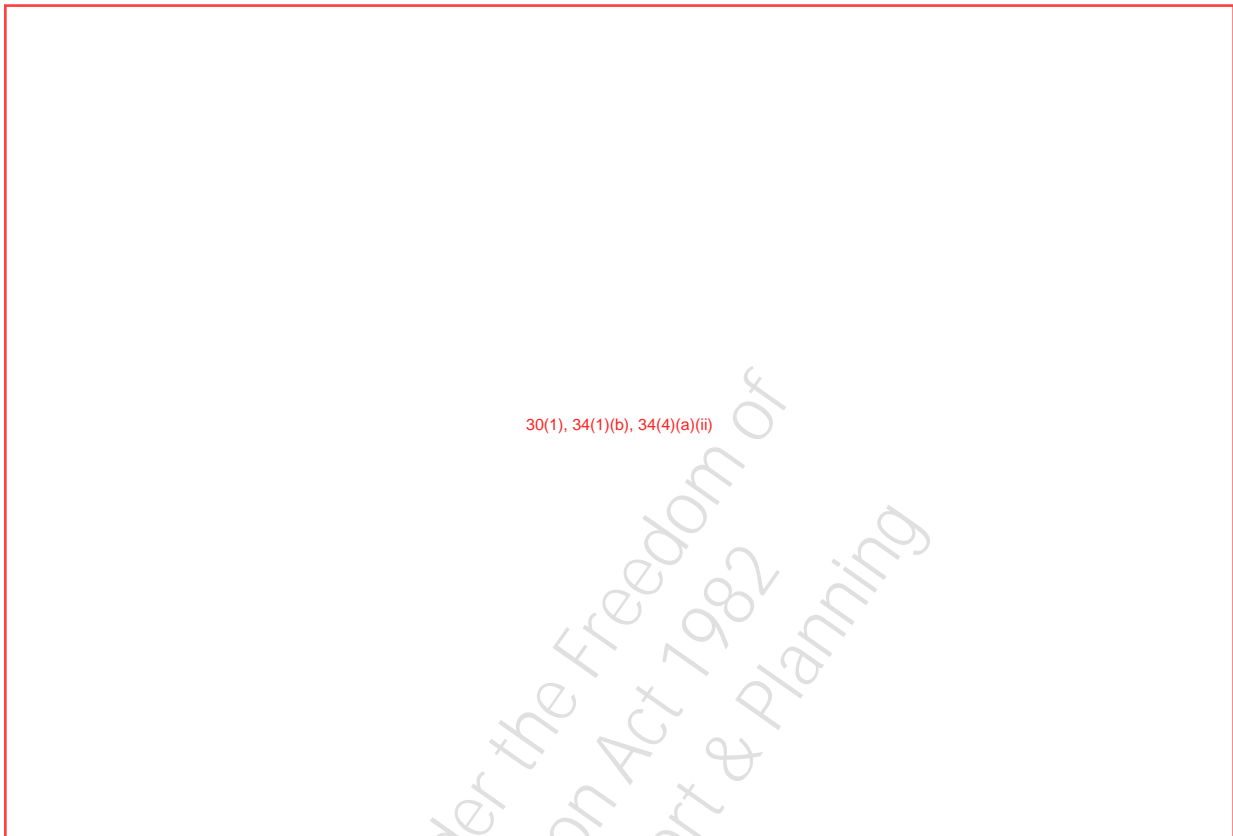
#### 3.4 About the DDL

The DDL will be accessible through the customer's Service Victoria digital wallet in the Service Victoria app. The app will allow the user to display the image of the driver licence for an 'at a glance' proof of age but also to generate a QR code that will be scanned by checkers to verify the licence status.

The DDL will contain features, such as holograms, animated logo, manual refresh, display of the last refreshed date and time and a watermark, that are digitally equivalent to the features that indicate a plastic licence is legitimate. DDLs will also have additional security features:

- DDLs are protected by the user's phone password (if used) and is only accessible by logging into the Service Victoria app via a user login, biometric identification, or 6-digit PIN.

### 3. PROJECT DESCRIPTION



Service Victoria is also considering several possibilities to offer selective disclosure to the user, which means that the app will allow the user to share only the relevant information from the DDL – for example, proof of being over 18 years old for entering a licensed venue, entitlement to drive etc. The QR Code will then contain the data fields that the user chose to share with the checker.

Law enforcement checkers will have an authority app to check the QR Code. Non-law enforcement checkers will access the QR Code reader from the regular, publicly distributed Service Victoria app.

### 3.5 Participants in the DDL Project MVP

This section sets out the participants in the DDL project at the MVP pilot phase.

#### 3.5.1 The DoT

The DoT operates and coordinates Victoria's transport network, the delivery and upgrade of transport infrastructure, as well as the reforms to road safety policy, regulatory and legislative environment. The DoT will remain the owner of the registration and licencing (R&L) data.

### 3. PROJECT DESCRIPTION

The DoT is also the policy owner of driver licensing policy. All the elements that relate to licence information, entitlement to drive, safety and roads will stay with the DoT. The user's licence features and potential changes (e.g., addition of a licence, expiration, suspension) are managed on the DoT's side, and Service Victoria only reflects those changes through the DDL. For the purposes of implementing the DDL, the DoT is providing and operationally supporting the APIs and data change notifications to Service Victoria.

#### 3.5.2 Service Victoria

Service Victoria was created by the Victorian Government to modernise Victorian customer's online government services and make it easier for people to complete more online services more often from the comfort and safety of their own homes. Customers can get to more than 80 government services through Service Victoria with more added all the time.

Service Victoria is responsible, with input from the DoT, for the solution delivery, the DDL product and design, and will host the DDL in its digital wallet within the Service Victoria mobile app. It is in charge of the maintenance of the app and ensuring that the right security, privacy and compliance features are in place. Service Victoria is also responsible for the communications with customers and will provide a digital channel for customer feedback about the DDL and pass complaints in relation to the DDL to the DoT.

Over time, the Service Victoria digital wallet is expected to include a wide range of Victorian government licences and permits.

#### 3.5.3 Checkers – Victoria Police

Service Victoria and the DoT have had initial consultations with VicPol. VicPol is also part of an advisory group with the DoT. The DoT has invited Service Victoria to participate in the advisory group to implement the DDL in 2022.

The external regional pilot will be used to test the efficacy of, and seek feedback on, the authority app already available to check the QR Code. However, as noted, for the MVP the DDL is supplementary to a plastic licence IIS understands VicPol will only be checking the DDL as an initial check and will also verify the physical driver licence through the LEAP (Law Enforcement Assistance Program) database. The pilot will help identify any needed modifications of police processes if/when the DDL is a legally binding driver licence.

#### 3.5.4 Checkers – other, including pubs and clubs

For the external pilot, a number of participating businesses and licenced venues have been selected in Ballarat, such as:<sup>2</sup>

- National Retailers – click & collect

---

<sup>2</sup> See 050522.DDL.Pilot.Scope.UC.Roadmap



### 3. PROJECT DESCRIPTION

- Licensed venues such as bars, pubs, nightclubs and restaurants
- Hotels
- Petrol service stations
- Supermarkets and grocery stores
- Convenience stores
- Tobacco retailers.

#### 3.5.5 Victorian citizens using a DDL

The external pilot will concern the population of the regional centre of Ballarat, only for drivers aged 21 and above and with a full licence including car, motorcycle, light, heavy vehicles. Service Victoria estimates that the early adopters of the DDL will represent around 25% of the Ballarat population over 21 years old with a full licence, which means around 25,056 users for the external pilot.

After the MVP, the DDL will be extended to all licence holders including probationary drivers and learner drivers in further stages of the project.

### 3.6 Nature of systems and information flows

#### 3.6.1 Key system components

##### 3.6.1.1 The DoT

The main DoT systems involved for the DDL are:

- 
- 

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

### 3. PROJECT DESCRIPTION

30(1), 34(1)(b), 34(4)(a)(ii)

#### 3.6.1.2 Service Victoria

To build the DDL, Service Victoria is reusing existing infrastructure previously used within Service Victoria. An advantage here is that Service Victoria has confidence in the systems, including because a number of components have already gone through security audits.

The Service Victoria platform hosts the app. The customer must download the app on their device and create a Service Victoria account to be able to generate a DDL and hold it within their digital wallet.

#### 3.6.1.3 Licence holders

Licence holders will use their own devices to set up, or use, a Service Victoria account, and to add a DDL to the Service Victoria digital wallet within the mobile app.

### 3.6.2 Kinds of information involved

#### 3.6.2.1 Personal information

The kinds of personal information to be shared by the DoT is the same as what currently appears on the plastic licence. This is:

- Full name
- Date of birth
- Address
- Signature
- Photo
- License number
- License expiry date
- Licence type (car/bike/dual)
- Licence proficiency (full/probationary)
- Licence category (heavy vehicle categories)
- Licence condition code.

### 3. PROJECT DESCRIPTION

The DDL QR Code will also display information which, if the differential display is included, will vary depending on the customer's preferences. The aim is that more sensitive licence information will only be available under the photo of the licence when activating the toggle button 'show licence details' (e.g., licence type, condition). If the DDL user chooses to share only name and age with a non-law enforcement checker, this is what will display to the checker.

Subject to product decisions, the DoT will also share information that will allow the following information to be displayed via the QR Code:

- Show the customer's full driver licence details (including status)
- Prove the customer's identity.
- Prove the customer is over 18.

#### 3.6.2.2 Sensitive information and health information

The DoT will also share some limited medical information about licence holders. This is in the form of conditions included on driver licences (e.g., use of glasses when driving). While the conditions are not described, the meaning of the codes is readily available. IIS considers the codes that are associated with a medical condition meet the definition of health information.

The DoT will also share biometric information with Service Victoria in the form of the licence photo and signature. Biometric information is not explicitly contained in the definition of sensitive information in the PDPA. However, it is considered sensitive information under the *Privacy Act 1988* (Cth) and OVIC advises organisations to consider treating biometric information as 'delicate information' and to handle it cautiously.<sup>3,4</sup>

#### 3.6.3 Overview of information flows

At a high level, the arrangements for the DDL are expected to involve the following:

- The DoT would integrate its R&L data with Service Victoria's DDL 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)
- As noted, Service Victoria will be using its existing infrastructure and processes for Service Victoria accounts and digital wallet to support the DDL. It will add a QR code generation process. Customers will use an existing Service Victoria account, or set one up, requiring consent-based identity verification (at a level of assurance two in accordance with its Identity Verification Standards).<sup>5</sup> Service Victoria is designing its system to allow for secure 'blind' pass through of data between the DoT to a customer's device. It will 'see' personal information only at the QR code generation step and will not retain any personal information, including in audit logs.

<sup>3</sup> Please refer to the definition given by OVIC: "*Delicate information* refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regard as requiring a higher degree of protection.", available at [https://ovic.vic.gov.au/book/key-concepts/#Sensitive\\_and\\_delicate\\_information](https://ovic.vic.gov.au/book/key-concepts/#Sensitive_and_delicate_information)

<sup>4</sup> See <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>

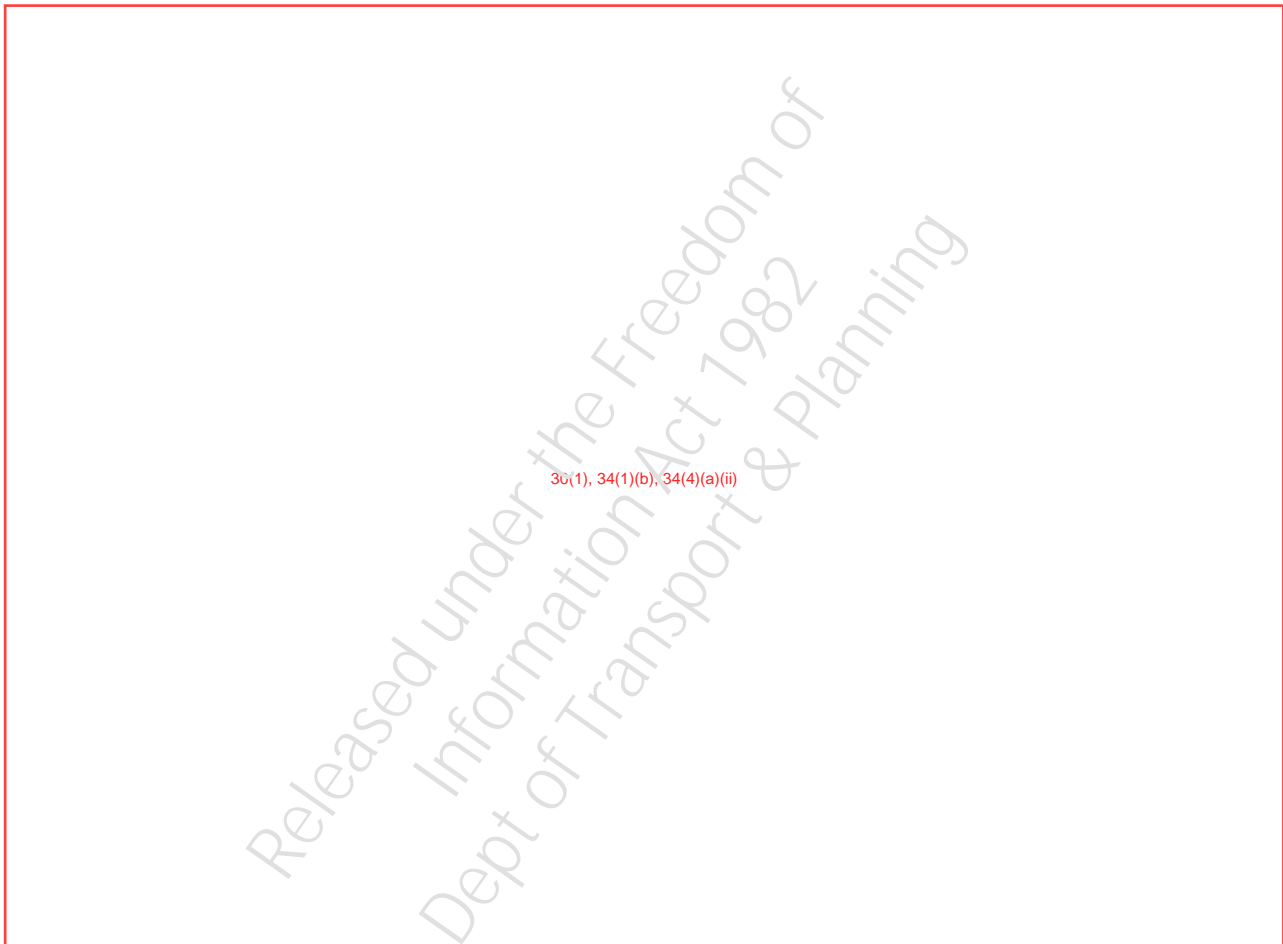
<sup>5</sup> See <https://service.vic.gov.au/about-us/service-victoria-identity-verification-standards>

### 3. PROJECT DESCRIPTION

- Customers can choose to show their DDLs to checkers (law enforcement agencies, or businesses seeking proof of identity or age).

The following diagram provides an overview of the architecture and information flows for the DDL from the DoT's perspective.

Diagram 1 – The DoT Digital Driver Licence Conceptual Architecture



The following section describes in more detail the information flows relating to the creation of a Service Victoria account and the creation of a DDL in the Service Victoria app. It also describes the information flows when a QR Code is generated and validated using the Service Victoria app (both by the customer and the checker).

### 3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
Log into the app/create an account	
<p>The customer logs into the app.</p> <p>If the customer doesn't have an account, they create one and start by entering the email address, password, first and second name in required fields. Customer creates a 6-digit PIN and can set up biometric authentication (such as their face or fingerprint).</p>	<p>If an account is created, email address and mobile phone (if provided) are verified via the use of a one-time password.</p>
Verify identity with choice of ID	
<p>The customer provides consent to verify their identity at a level of assurance two (LOA2). This requires the customer to provide two satisfactory identity documents from the list below:</p> <ul style="list-style-type: none"> <li>● a full Australian birth certificate; OR</li> <li>● a full Australian passport; OR</li> <li>● a foreign passport with a valid Australian visa; OR</li> <li>● an ImmiCard; OR</li> <li>● an Australian Citizenship Certificate; OR</li> <li>● an Australian driver licence; OR</li> <li>● a Medicare card.</li> </ul> <p>If the user has an account with an existing electronic identity credential (EIC) at Level of Assurance (LOA2) or above, Service Victoria validates the identity.</p>	<p>The customer undergoes identity verification. <span style="border: 1px solid red; padding: 2px;">(1)(b), 34</span></p> <div style="border: 1px solid red; padding: 10px; margin-top: 10px;"> <p style="text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
<p>The user is presented with the choice to create an ongoing Electronic Identity Credential that will be valid for 10 years.</p>	<p>The customer's full name and date of birth are retained for 10 years if the customer consents to creating an ongoing Electronic Identity Credential.</p>

### 3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
Add the DDL to the wallet	
<p>In the 'My Wallet' tab of the app, there will be an 'Add Driver Licence' button. User taps on this.</p> <p>At this point the customer provides their consent to verify their Australian driver licence.</p>	<p>This will trigger the normal flow in the back end for when there has been a request to add something to the wallet.</p> <div data-bbox="764 582 1353 707" style="border: 1px solid red; padding: 5px; text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</div>
<p>The customer is presented with a screen with their first name, last name and DOB, and empty fields requiring them to enter their driver licence number and expiry date.</p>	<p>All this information will be sent to the DoT via an API for verification purpose. <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <div data-bbox="764 822 1375 1055" style="border: 1px solid red; padding: 5px; text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</div> <p>Upon verification, the personal information is encrypted <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <div data-bbox="764 1160 1375 1285" style="border: 1px solid red; padding: 5px; text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</div>
<p>The customer can now access the DDL from the Service Victoria wallet.</p>	<div data-bbox="764 1312 1375 1438" style="border: 1px solid red; padding: 5px; text-align: center; color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</div>

### 3. PROJECT DESCRIPTION

Steps for the user	Back-end processes
QR Code generation and validation	
<p><b>Generating a QR Code:</b></p> <p>Subject to ongoing product development of the DDL, the user will be given the choice to decide on different sharing options. This will allow them to determine how much of their driver licence information they'd like to show to non-law enforcement checkers.</p>	<div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
<p><b>Validating a QR Code:</b></p> <p>Law enforcement and businesses that require proof of age or proof of eligibility to drive will be able to scan the QR code to verify its validity and to see the licence information (what is shown will depend on the policy about differential display, and then on what the DDL user chooses to display)</p>	<div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>

## 3.7 Legal framework

### 3.7.1 Victorian laws

The DDL project must comply with the following relevant laws.

#### 3.7.1.1 Privacy and Data Protection Act 2014

The *Privacy and Data Protection Act 2014* (PDPA) regulates the handling and protection of personal information by Victorian public sector organisations. Organisations subject to the PDPA must comply with the Information Privacy Principles (IPPs) that contain requirements across the information lifecycle. Part 4 of the PDPA gives the Victorian Information Commissioner the power to prescribe security requirements pertaining to public sector information and information systems through the Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS).

### 3. PROJECT DESCRIPTION

#### 3.7.1.2 Health Records Act 2001

The *Health Records Act 2001* (HRA) and its Health Privacy Principles (HPPs) regulate the collection, handling and protection of health information, which includes information or opinion about the physical or mental health or disability of an individual.<sup>6</sup>

#### 3.7.1.3 Road Safety Act 1986

The *Road Safety Act 1986* (RSA) is the main piece of legislation that regulates the use of roads, registration of vehicles and driver licensing in Victoria.

The DoT and Service Victoria have had a Service Agreement since 2017. For the DoT to disclose the data to Service Victoria, the DoT and Service Victoria also had to enter into an Information Protection Agreement (IPA) in accordance with section 90N of the PSA. No legislative changes to the RSA are needed for the MVP, as the recent amendments of the RSA and the *Service Victoria Act 2018* are sufficient to deliver the pilot. In the longer term, changes to RSA might be necessary to incorporate digital services.

Part 7B of the RSA applies to Service Victoria because it has requested access to the driver licence information held by the DoT where the information may identify an individual or allow an individual's identity to be ascertained. Part 7B contains the protective framework for relevant information, including the allowed purposes for use and disclosure of relevant information, the exceptional circumstances for the use and disclosure of relevant information, the uses of relevant information for verification purposes, etc.

#### 3.7.1.4 Service Victoria Act 2018

The *Service Victoria Act 2018* provides for the delivery of Government services to the public by Service Victoria and provides a regulatory framework for the provision of identity verification functions by the Service Victoria CEO. Importantly, the Act establishes that the Service Victoria CEO must comply with identity verification standards when verifying identity. These standards are set out separately to the legislation and provide a consistent and secure identity verification framework for people transacting with the Victorian Government through Service Victoria. Among other things, the *Service Victoria Amendment Act 2022* added new provisions supporting digital delivery of Victorian licences.

#### 3.7.1.5 Charter of Human Rights and Responsibilities Act 2006

The *Charter of Human Rights and Responsibilities Act 2006* (the Charter) is a Victorian law that sets out the protected rights of all people in Victoria as well as the corresponding obligations on the Victorian Government. No issue related to the Charter have been identified for this PIA.

---

<sup>6</sup> The HPPs are substantially similar to the IPPs. For the purposes of our privacy analysis in Section 5, IIS has focused on the IPPs.



### 3. PROJECT DESCRIPTION

#### 3.7.1.6 Road Safety (Drivers) Regulations 2019

Regulation 63 of the Road Safety (Drivers) Regulations 2019 describes the details that driver licence or learner permit documents must contain, including the identification number, the person's first name, second and third initials (if any) and family name; a photograph of the person; the person's residential address; the person's date of birth; a reproduction of the person's signature; the category or categories of driver licence; its expiry date; and the code of any condition to which the licence or permit is subject.

### 3.8 Project governance

In November 2021, the Interdepartmental Committee (IDC) endorsed preliminary detailed scoping work to support a MVP release strategy.

The DDL project is a collaboration between DoT and Service Victoria. At project initiation Service Victoria provided DoT with a delivery agreement. This agreement specified the scope and timeline for work. The agreement has been unable to be finalised as feedback from DoT is outstanding.

In addition to this, the governance arrangements for this development phase of the project have included:

- Ministerial oversight via monthly ministerial meetings
- Steering committee with senior staff from Service Victoria and the DoT
- Working groups sitting under the steering committee with weekly meetings.

These arrangements are now moving to a more formal partnership arrangement with the DoT, taking account of the fact that the authorising governance will be coming from Cabinet, as well as the DoT's proposed Joint Venture (JV), which will see modernisation of its systems and processes.

The formal governance arrangements for the next stages of the DDL project will be subject to legislative requirements, outlined above, including the IPA.

The arrangements include:

- Ministerial oversight
- A Memorandum of Understanding (MoU) between Service Victoria and the DoT, setting out overall principles on how the relationship works and a high-level governance framework
- Operating service commitment
- Transaction journey documents
- Delivery agreement
- Information Protection Agreement.

These documents and processes set expectations and respective roles and responsibilities, including with respect to privacy.

## 4. APPROACH TO RISK ANALYSIS

IIS understands the MoU and Information Protection Agreement have now been signed. Service Victoria and the DoT are working through other relevant documents and more detailed requirements, including with respect to privacy. These will need to be finalised before the DoT provides R&L data to Service Victoria for the DDL. IIS also understands that the structure of project steering committee and related working groups and consultative processes will continue.

### 4. Approach to risk analysis

In undertaking this PIA, IIS considered:

- The IPPs in the PDPA
- Guidance materials published by the OVIC and the CAiC
- Privacy good practice stemming from IIS's knowledge and experience.

The PIA focuses on privacy risks that are introduced or heightened by the DDL project, rather than privacy risks for existing processes to issue and use driver licences.

This section assesses the project's residual privacy risk level, by weighing the inherent privacy risks against the existing privacy positive aspects.

The following section discusses the project's privacy issues and risks identified in detail and makes recommendations to mitigate the risks.

#### 4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks. Inherent privacy risks arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential (including value) for, and consequences of, misuse
- The range of people from whom the information may be collected
- The context in which personal information is handled – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the project
- The extent to which information is accessed or handled by third parties
- The likely community and/or media interest in the privacy aspects of the project.

Taking account of these factors, IIS considers

30(1), 34(1)(b), 34(4)(a)(ii)

), 34(1)(b), 34(4)(c)

- The project will involve the transfer of R&L data – which is considered very valuable and sensitive – from the DoT to Service Victoria to provision DDLs.

#### 4. APPROACH TO RISK ANALYSIS

- The DoT will be combining and transferring driver images as well as R&L details. The DoT considers that this adds to the project risks. IIS agrees this is a risk to the extent that it could be compromised (even if very unlikely).
- The project is in its initial phases and is subject to some uncertainty. Service Victoria has undertaken considerable consultation and design work in collaboration with the DoT. Its future directions are now subject to formal agreement and approval on matters including final design, security and governance, and on the outcome of two planned pilots.

- 30(1), 34(1)(b), 34(4)(a)(ii)

- The DoT is seeking further information from Service Victoria so that it can assess its security culture and risk management in the context of the DDL.
- Service Victoria's design has taken account of possible security risks for DDL users. However, DoT is currently conducting further security assessment processes. These should be concluded before the project proceeds for the external pilot.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including how checkers can interact with their devices, or handle personal information displayed via the DDL – can have a significant impact on them and jeopardise uptake of the solution.

Not all of these matters, 

30(1), 34(1)(b), 34(4)(a)(ii)

 are within scope for this PIA, but to the extent they may impact on privacy risks, we have considered them.

## 4.2 Positive privacy aspects

IIS considers that the DDL project has important positive aspects that support privacy and minimise the inherent risks associated with the project. These are outlined below:

### Positive privacy aspects with the project/solution design

- Service Victoria has followed the key privacy enhancing strategy of data minimisation – it will handle minimal personal information and will not retain any such information. In particular:
  - When the DDL has been added to the Service Victoria wallet, the only thing stored in Service Victoria's platform is a linking key 

34(1)(b), 34(4)(a)(ii)

 in the wallet database. This indicates that the user has a driver licence in their wallet, and the platform uses that linking ID to get the driver licence information from the DoT.
  - The path through Service Victoria's platform from the DoT to the app is automated, no licence information is stored, and no Service Victoria personnel will have access to it as it passes through the platform. Service Victoria specified that there are no 'dead letter queues' or any other place where information may inadvertently be stored.

## 4. APPROACH TO RISK ANALYSIS

- The DDL project design appears to avoid the risk of a new digital footprint, in that neither Service Victoria or the DoT will have any detailed records that would enable them to track when, or to whom, a customer presents their DDL for checking. The DoT will keep an audit log, which would allow it to identify and investigate a transaction.
- The DDL does not rely on the creation of duplicate stores of personal information. b0(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) This means the DoT data remains the single 'source of truth' for driver licence information.
- The device used to display the DDL only holds the image of the licence. The validated details in the QR code are generated by a call to the DoT, and, following validation, are only available for display without refresh for a limited period (the timeframe is yet to be decided but likely in the order of minutes).
- Service Victoria and DoT have indicated a commitment to privacy and appear to have this in mind as the project design is finalised and as it proceeds to implementation. This includes having appropriate governance arrangements in place to support privacy requirements.
- The arrangement between DoT and Service Victoria is governed by a MoU and IPA (as required under Part 7B of the RSA). These documents contain the roles and responsibilities of both parties and in particular the privacy and security obligations.

### Privacy advantages for DDL users over the existing plastic driver licence

- The DDL is more secure in that it is protected by device and Service Victoria app security measures, including password or PIN protection.
- The DDL includes a range of other security features and further work is being undertaken to identify if other measures are needed.
- If an individual's device is lost or stolen, this does not mean the information is lost. A user can, with relative ease, add their DDL to another device. If a DDL is reported stolen, notification from the DoT can be reflected in the QR Code.
- A customer's DDL can be validated in real-time. This means data can be instantly verified using either the authority app, or by scanning the QR code displayed on the DDL within the Service Victoria app.
- Subject to policy decisions, DDL users will have some choice about what information they display to checkers.

### 4.3 Residual privacy risk level

IIS has not identified any show-stopping privacy issues for the project. Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. Rather, the issues identified arise in the context of the project stage and the complexity of the project environment.

In summary, given the project's early stage, with a number of important issues to resolve, IIS considers the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to the decisions made about security levels, governance, etc. and to systems being in place.

## 5. FINDINGS AND RECOMMENDATIONS

# 5. Findings and recommendations

This section discusses relevant privacy risks and issues that IIS has identified during the PIA.

The recommendations focus on mitigating privacy risks and improving practice during the further development of the DDL. For each recommendation, we have suggested who would be responsible for carrying out the recommendation (the DoT or Service Victoria, or both).

## 5.1 IPP issues or risks

A high-level analysis of phase 1 of the DDL project against the IPPs is at [Appendix B](#). IIS considers that the DDL project would be mostly consistent with the IPPs. For example:

- The project operates within the existing legal framework – while DoT is considering whether it is authorised to disclose R&L information for the MVP external pilot, IIS assumes this will be resolved before the pilot proceeds.
- Service Victoria will be authorised to collect and handle limited, generally encrypted, personal information consistent with the Service Victoria Act 2018.
- Anonymity is not practicable.
- The project will operate within Victorian borders.

The main IPPs where IIS has identified issues are in relation to openness, security, and access and correction, and privacy complaint handling.

### 5.1.1 Transparency – IPP 1 and IPP 5

Transparency provisions in the IPPs aim to allow individuals to make informed choices about providing information or using a service and to have a general understanding of how information about them is being handled. Transparency is both a matter of compliance as well as key to building public confidence and trust in the DDL. The IPPs provide two transparency mechanisms:

- Specified details provided at the point personal information is collected (IPP 1.3)
- General information available about the type of personal information agencies collect and hold and how it is managed (IPP 5.1).

#### 5.1.1.1 Privacy collection notice and privacy policy

At the time of writing this PIA, IIS understands that both the DoT and Service Victoria are undertaking work on their privacy collection notices and privacy policies. They have indicated they would adopt a best practice approach, for example using layered notices.

In regard to the collection notice, IIS notes that Section 12.1 of the MoU states that collection notices will be provided by the DoT. IIS has been informed that a layered approach to the notices will apply:

## 5. FINDINGS AND RECOMMENDATIONS

- Service Victoria's collection notice will refer to the collection of data necessary to add a DDL within the Service Victoria app
- The DoT's collection notice will refer to the collection and use of R&L information.

Service Victoria shared with IIS a draft collection notice for the DDL pilot. IIS found the collection notice to be clear; we did not identify any issues in term of the requirements of IPP 1.3.

IIS understands Service Victoria will continue to develop its privacy materials in consultation with DoT, and following the established Service Victoria style guide and patten (in accordance with the MoU).

Noting that both DoT and Service Victoria are working on privacy materials,

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

it is

important that there is a clear process for coordinating and approving the privacy materials across the DDL project. In addition, the privacy messages delivered by both DoT and Service Victoria should be consistent.

IIS considers, for example, that Service Victoria would need to have privacy information about the Service Victoria account, app, and the DDL on its website and also at relevant places in the app. It will be particularly important that the DDL app makes clear what personal information will be shared when an individual presents their phone to a checker. IIS also considers the more general communications for the MVP pilots should address the question of DDL processes where a venue would currently take a copy of a plastic licence. For example, it might be that customers would be encouraged to offer both the DDL and the plastic licence in these circumstances.

In respect to Service Victoria's privacy policy, IIS encourages Service Victoria to include

30(1), 34(1)(b), 34(4)(a)(ii)

section on the information handling for DDLs, just as it has done so for the COVID-19 digital certificate. This might cover, for example, information about:

- Collection and handling of information for identity verification
- Activity logs
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential checker handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 1 – Ensure that project agreements and governance arrangements provide for a process for ensuring that privacy messages are consistent and adopt best privacy practice

Project agreements and governance arrangements that give effect to the MoU should have processes to ensure that privacy messages delivered by the DoT and Service Victoria are consistent, comprehensive and adopt best practices approaches. The governance processes should make clear who is responsible for signing-off on privacy materials and monitoring their use.

**Who:** Both Service Victoria and DoT

**Timeframe:** For MVP and ongoing

### Recommendation 2 – Service Victoria and DoT privacy policies to include comprehensive DDL information

Service Victoria's and the DoT's privacy policy should include comprehensive DDL information.

Service Victoria's privacy policy should include an additional 'extra privacy information' section on the information handling for DDLs, which should cover matters such as:

- Collection and handling of information for identity verification
- Activity logs
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential checker handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

**Who:** Service Victoria and DoT

**Timeframe:** For MVP and ongoing

#### 5.1.1.2 Public communications and education

In addition to the specific requirements in the IPPs, active public awareness and education for DDL users and checkers will support transparency about the project, and support individuals' ability to exercise their privacy rights and to use a DDL safely.

IIS understands that a public communications strategy of this sort is planned but is not yet developed. Both the DoT and Service Victoria noted the importance of tailoring communications to the audience, including by using plain English and appropriate language levels.



## 5. FINDINGS AND RECOMMENDATIONS

IIS considers it is important that the public communications provide guidance to DDL users on privacy and security aspects of the DDL and also to checkers on how they should validate the DDLs. The emphasis in the guidance for both users and checkers should include explicitly informing them that the licence image on the Service Victoria wallet is simply a replicated image and that the verified licence details are encrypted within the QR Code.

Service Victoria and the DoT both have a role to play to ensure that this message gets across so that DDL users are showing their QR code (not just the licence image) and that checkers are validating the QR code and not simply sighting the licence image.

Individuals should have adequate information on what sharing options are available for the DDL, how to generate the QR Code, what the process is when allowing checkers to sight their QR code and what their rights are. With regard to checkers, it is important that they are aware what the rules are surrounding validating an individual's DDL.

The information could be made available on Service Victoria and the DoT's website and in FAQs.

### Recommendation 3 – Public communications should provide comprehensive privacy and security information

As a matter of best practice, deploy a public communications strategy to support individuals and checkers to understand their rights and responsibilities with regard to the use and validation of a DDL. Such a strategy should:

- Ensure that public are aware of the difference between the licence image and the QR Code.
- Support individuals' ability to exercise privacy rights and use a DDL safely
- Recommend best practice for checkers when validating DDL
- Ensure messages are consistent and comprehensive across all channels and between Service Victoria and the DoT (and the JV partner) where relevant
- Ensure that FAQs are easily accessible and cover likely privacy questions including potential security risks and the role and the process for checkers

**Who:** Both Service Victoria and DoT

**Timeframe:** For MVP and ongoing

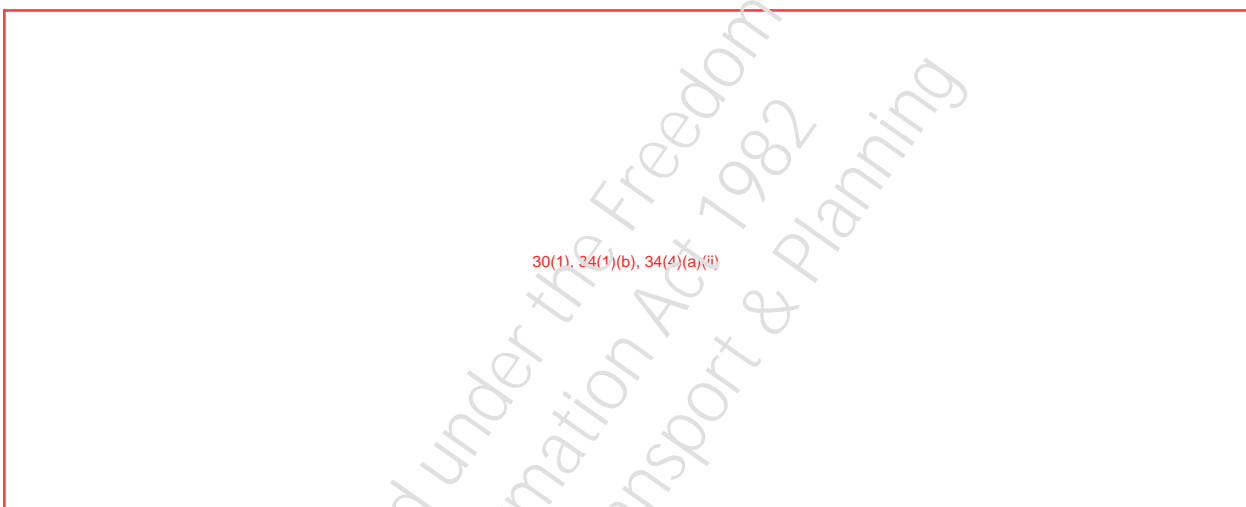


## 5. FINDINGS AND RECOMMENDATIONS

### 5.1.2 Security – IPP 4

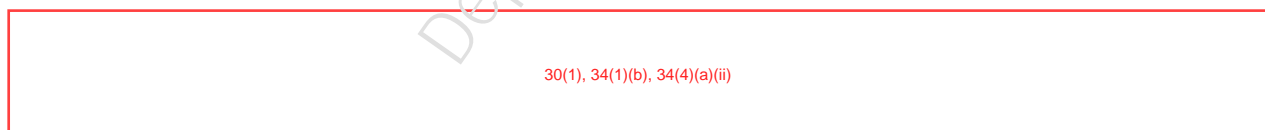
IPP 4 requires agencies to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. The DoT and Service Victoria will also be subject to the VPDSF and VPDSS. The VPDSS prescribes a minimum set of mandatory requirements across all security areas including governance, information, personnel, ICT and physical security. The VPDSF provides direction to Victorian public sector agencies or bodies on their data security obligations.

IIS notes that the DoT treats disclosure of R&L data to Service Victoria as though it were a disclosure to a third party; its security due diligence measures take account of this context.



It is outside the scope of the PIA to assess the technical security of the DDL. However, IIS sought an understanding of the security approaches to date and the further steps needed.

#### 5.1.2.1 System security



Both Service Victoria and the DoT have noted a number of design features for the project that aim to mitigate the risks. Both also outlined their security approaches and noted specific steps they have taken, or are planning to take, to identify and manage security risks for the project. The DoT advised that the completion of the IVA and the Protected designation will now call for rigorous assessment of systems and processes to determine what more is needed.

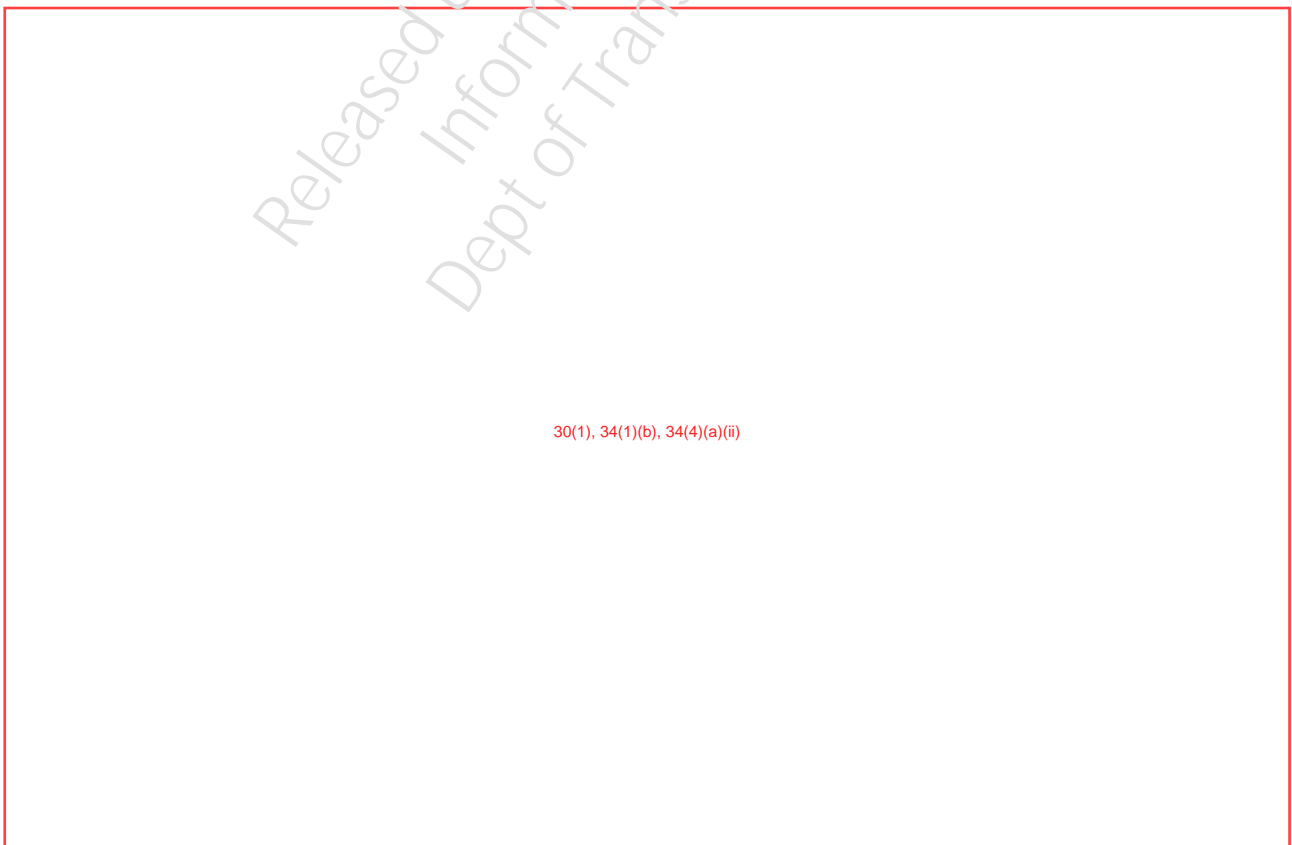
## 5. FINDINGS AND RECOMMENDATIONS

Security actions that are relevant for this PIA include:

- **Incorporation of Security by Design in the development of the DDL**



- **Security assessments**



## 5. FINDINGS AND RECOMMENDATIONS

30(1), 34(1)(b), 34(4)(a)(ii)

### Recommendation 4 – Ensure decisions on security posture are made before the external pilot and are reflected in DDL customer information

The DoT and Service Victoria to ensure decisions on security including data classification and LOA are made before the external pilot and are clearly reflected in information for DDL users. The approaches should be managed to avoid privacy gaps or weaknesses, and be balanced so that they are practical and workable from individuals' perspectives.

**Who:** Both Service Victoria and DoT

**Timeframe:** For MVP and ongoing

### Recommendation 5 – Record DDL related privacy risks on risk register

Ensure that project risk processes include risks to individuals using a DDL and that these risks are included in project risk registers and monitored.

**Who:** Both Service Victoria and DoT

**Timeframe:** Before the DDL design and go-live decisions are finalised

#### 5.1.2.2 Security for users of the DDL

30(1), 34(1)(b), 34(4)(a)(ii)

## 5. FINDINGS AND RECOMMENDATIONS

Features it noted included that:



---

<sup>7</sup> See <https://www.service.nsw.gov.au/privacy-and-digital-licences-and-credentials#licence-or-credential-checkers-handling-your-phone>

## 5. FINDINGS AND RECOMMENDATIONS

### Recommendation 6 – Clarify and communicate requirements for the handling of individuals devices for DDL checking

Clarify whether checkers may take an individual's device when checking a DDL. Include clear information on this issue in communications for the pilot for individuals using DDLs and for checkers including VicPol. Consider legislative change if needed to ensure that individuals do not need to hand over their devices during a DDL check.

**Who:** DoT

**Timeframe:** For MVP and ongoing

#### 5.1.3 Access and correction – IPP 6, and privacy complaint handling

Both Service Victoria and the DoT agree that processes for correction as well as complaint handling will have to be worked out to ensure the customers are able to have their issues attended to by the appropriate entity. IIS has been informed that it will be a shared responsibility to rectify issues around the DDL. The DoT will be responsible for providing the licence information and related information about its validity, while Service Victoria will also need to field queries as the DDL will be on the Service Victoria wallet.

The MoU includes complaint handling principles to which the DoT and Service Victoria must adhere. It specifies that both parties will assist each other and cooperate to resolve any complaints or issues and that complaints will be referred to the responsible party.<sup>8</sup> IIS understands that Service Victoria has extensive experience in managing customer services issues and complaints on behalf of its agency partners, including the DoT.

While IIS acknowledges this is not a new issue for Service Victoria, we encourage the DoT and Service Victoria to ensure there is a streamlined 'no-wrong-door' approach to receiving, and assisting individuals with, privacy queries and complaints related to DDL. We note that a draft Operating Service Commitment which sets out the standards for jointly delivering customer service transactions has been developed.

Overall IIS considers that Service Victoria and the DoT have strong measures in place to deal with privacy enquiries and complaints, and we encourage them to continue monitoring the procedures to ensure that they stay fit for purpose.

---

<sup>8</sup> Section 8.3 of MoU – Complaint Handling Principles

## 5. FINDINGS AND RECOMMENDATIONS

### 5.2 Governance

#### 5.2.1 Project governance

As noted, the DDL project is in its initial phases and is subject to some uncertainty, for example in relation to aspects of the security approach. In addition, while Service Victoria has had privacy as a clear focus in the design and development work to date, the process to maintain this focus did not seem clear. The project governance arrangements have also changed somewhat to reflect that the project is now subject to Cabinet decisions and oversight, and to reflect DoT's (proposed) engagement of a JV partner to deliver some functions.

IIS understands that the overarching MoU has now been signed. Detailed agreements, including the DDL transaction journey, that will set out the arrangements between the DoT and Service Victoria are now being developed but are not yet finalised. Privacy requirements will be included. However, the nature of the requirements, and processes for ensuring a coordinated best practice approach and for privacy to remain a priority in implementation, evaluation, and monitoring phases are not yet clear.

#### Recommendation 7 – Ensure project governance arrangements include clear privacy roles and responsibilities, including for monitoring privacy outcomes

Service Victoria to ensure and document a privacy approach that makes clear who is responsible for privacy sign-off for the project, and that monitoring privacy outcomes is included in its project implementation and evaluation plans.

The DoT and Service Victoria to ensure detailed agreements and ongoing project governance processes include clear privacy requirements and responsibilities for the project, and a comprehensive and coordinated approach to ensuring privacy objectives are met.

**Who:** Both Service Victoria and DoT

**Timeframe:** For MVP and ongoing

#### 5.2.2 Privacy by Design (PbD) and future developments

As noted Privacy by Design has been a feature of the DDL project development to date. IIS encourages both Service Victoria and the DoT to continue this approach. It will remain relevant as the MVP is settled and as the DDL is developed further. Particular areas for future privacy focus includes:

- Allowing for differential display of DDL details, so that individuals can present only relevant information to a checker – this feature is planned however details are yet to be decided.
- If a notifications feature is introduced allowing, to the extent possible, for individual choice about whether or not to receive notifications.

## 5. FINDINGS AND RECOMMENDATIONS

- The possible display of licence status and demerit points. Both require further in-depth analysis around policy implications of formal notices/notifications in a digital environment. Where possible, individual choice should also be a key consideration.
- Potential for further privacy features, for example, including, if wished, a record on individuals' devices of which checkers have viewed their licence.

### Recommendation 8 – Continue to adopt PbD in the DDL's further development

Give priority to the inclusion of the differential display feature in the MVP, or as soon as is feasible thereafter.

Continue the current PbD approach for the DDL, including by conducting further PIAs before making changes to the DDL, for example notifications, or display of status or demerit points, which could impact on individuals' privacy.

**Who:** Both Service Victoria and DoT

**Timeframe:** Ongoing

Released under the Freedom of Information Act 1982  
Dept of Transport & Planning

6. APPENDIX A – METHODOLOGY

## 6. Appendix A – Methodology

### 6.1 PIA approach

IIS took the following steps to carry out the PIA:

- *Planning* with the DoT to confirm the approach, scope and deliverables of the PIA
- *Gathering information* by reading documents and meeting with personnel from the DoT and the Service Victoria
- *Analysing the information* against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy good practice
- *Identifying privacy risks* and developing ways to mitigate those risks
- *Developing a preliminary findings note* summarising the key findings from the information gathering stage
- *Drafting the PIA report* and providing this to the DoT for comment
- *Finalising the PIA report* following feedback from the DoT.

### 6.2 Documents reviewed

Documents reviewed	
<b>DoT documents</b>	
1.	[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
2.	Service Victoria Digital Driver Licence (DDL) Integration Recommended Solution, 4 May 2022
3.	DDL Risk Assessment v0.4, 31 March 2022
4.	Conceptual Architecture - Recommended Solution, 4 May 2022
5.	Card Production and image data Flow
6.	Request for Proposal, eServices Register, [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii) [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
7.	Memorandum of Understanding between Secretary to the Department of Transport and Service Victoria CEO Final, May 2022
8.	Information Protection Agreement with Service Victoria, 18 January 2022
9.	Renew Registration Transaction Journey - Final Schedule 2 Transaction Journey for Registration Renewal, 12 May 2022



6. APPENDIX A – METHODOLOGY

Documents reviewed
10. Schedule 2: Transaction Journey for Digital Driver Licence, 3 May 2022
11. Check Registration TJ - Final Schedule 2 Transaction Journey for Vehicle Registration Checking 12 May 2022
12. Memorandum of Understanding between Secretary to the Department of Transport and Service Victoria CEO, 3 May 2022
13. Information Protection Agreement Service Vic DoT 2021
14. Information Value Assessment – 2 June 2022
<b>Service Victoria documents</b>
15. Digital driver licence Pilot phases I & II, 21 March 2022
16. Digital driver licence Pilot phases I & II, 4 May 2022
17. A Digital Driver Licence for Victoria, Working with VicPol to implement a Victorian digital driver licence, 5 April 2022
18. Operating Service Commitment, 8 April 2022
19. Department of Transport Linking a Digital Driver Licence (Pilot) Service Victoria identity verification standards: level of assurance assessment and determination, 31 March 2022
20. Draft Privacy Collection Notice for Digital Driver Licence – 20220504
21. Digital Driver Licence - Transaction Journey (2022.05.16)
22. Operating Service Commitment - Final
23. Privacy complaints management procedure

### 6.3 Meetings held

Meetings held	Date
Kick-off meeting: <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● the DoT and Service Victoria personnel</li> </ul>	28 April 2022

6. APPENDIX A – METHODOLOGY

Meetings held	Date
PIA information gathering meeting – Legal (Service Victoria): <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● Service Victoria personnel</li> </ul>	9 May 2022
PIA information gathering meeting – IT and Security (Service Victoria): <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● Service Victoria personnel</li> </ul>	9 May 2022
PIA information gathering meeting – Products Team (Service Victoria): <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● Service Victoria personnel</li> </ul>	11 May 2022
PIA progress update meeting: <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● the DoT and Service Victoria personnel</li> </ul>	12 May 2022
PIA information gathering meeting – IT and Security (DoT): <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● the DoT personnel</li> </ul>	12 May 2022
PIA information gathering meeting – Legal (DoT): <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● the DoT personnel</li> </ul>	13 May 2022
PIA progress update meeting: <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● the DoT and Service Victoria personnel</li> </ul>	19 May 2022
PIA information gathering meeting – Legal (DoT): <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● the DoT personnel</li> </ul>	23 May 2022

6. APPENDIX A – METHODOLOGY

Meetings held	Date
PIA information gathering meeting – Victoria Police: <ul style="list-style-type: none"><li>• IIS personnel</li><li>• VicPol personnel</li><li>• the DoT personnel</li></ul>	24 May 2022
PIA progress update meeting: <ul style="list-style-type: none"><li>• IIS personnel</li><li>• the DoT and Service Victoria personnel</li></ul>	26 May 2022
PIA information gathering meeting – IT (Service Victoria): <ul style="list-style-type: none"><li>• IIS personnel</li><li>• Service Victoria personnel</li></ul>	26 May 2022

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

## 7. Appendix B – Assessment against the IPPs

The following table sets out IIS’s high-level assessment of the MVP against the IPPs. In making its assessment, IIS notes that internal pilot will be testing aspects of the DDL including the interface and will not include ‘real’ R&L data from the DoT. Subject to the DoT’s clarification of its legal authority, it will be providing R&L data for the external pilot. This will include some health information in form of licence codes. This would be subject to the HPPs in the HRA. IIS notes that the HPPs cover similar issues to the IPPs.

IIS notes that when Service Victoria is collecting data in the context of the DDL, for example, to validate a licence, it is doing so on behalf of the DoT. However, the DoT treats disclosure of R&L data as though disclosure to a third party.

IIS also notes that where its assessment has not identified specific issues for this PIA, that is not meant to indicate there is no privacy work to be done. IIS anticipates that usual privacy compliance and monitoring would occur.

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DoT
<p><b>IPP 1 – Collection</b></p> <p>An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation’s Privacy Policy.</p>	<p>The DDL involves a re-use of existing information the DoT holds, not a new collection for DoT.</p> <p>The MoU specifies that Service Victoria will be collecting personal information on behalf of the DoT (in process of loading DDL into the Service Victoria wallet, and in the process of creating/refreshing QR codes).</p> <p>The introduction of DDL is a new way of providing driver licences – it would be at least good practice to update both the DoT’s and Service Victoria’s privacy policies and to ensure privacy collection notices are available and relevant at point of use, for example within the Service Victoria app. The MoU states that Service Victoria must include or provide a link to a DoT collection notice in its app when people are seeking to add the DDL to their wallet.</p> <p>See discussion at <a href="#">Section 5.1.1</a>.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DoT
<p><b>IPP 2 – Use and disclosure</b></p> <p>Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual's consent, for a law enforcement purpose, or to protect the safety of an individual or the public.</p>	<p>The DoT's use of R&amp;L data for digital driver licence is consistent with the purpose of collection.</p> <p>IIS notes that for the purpose of the external pilot, the DoT is still considering whether it can disclose R&amp;L data. Subject to the DoT's view that the pilot can proceed within law, no privacy issues identified.</p> <p>The IPA also specifically states that Service Victoria undertakes that information shared by the DoT will only be used and disclosed for the purposes set out in the IPA (To provide an alternative digital customer channel for some vehicle registration and driver licensing activities and services of the Department of Transport including under the RSA). Section 90K of Part 7B of the RSA sets out the authorised use or disclosure. Section 90K(a)(vi) allows disclosure in relation to an intergovernmental agreement.</p> <p>No issues identified</p>
<p><b>IPP 3 – Data quality</b></p> <p>Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.</p>	<p>DDL should not diminish and may enhance data accuracy of driver licence information.</p> <p>Changes to driver licence details or status will be subject to pilots and roll-out and will be reflected in the DDL quickly.</p> <p>Service Victoria's design of the DDL is in such a way that it does not collect or hold identified personal information except in the limited context of the generation of the QR code. The one source of truth of driver licence information remains with the DoT.</p> <div style="border: 1px solid red; padding: 5px; text-align: center; color: red;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div> <p>No issues identified.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DoT
<p><b>IPP 4 – Data security</b></p> <p>Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.</p>	<p>The DoT and Service Victoria have in place detailed security management processes and have commenced or undertaken detailed security risk assessments for the DDL.</p> <p>At this point, there are some issues to work through – see discussion at <a href="#">Section 5.1.2</a>.</p>
<p><b>IPP 5 – Openness</b></p> <p>Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation’s Privacy Policy.</p>	<p>Both Service Victoria and the DoT will be updating their privacy policies to reflect DDL. From a privacy perspective, it will be important to ensure consistency and that individuals are easily able find relevant information to inform their decisions. See <a href="#">Section 5.1.1</a>.</p>
<p><b>IPP 6 – Access and correction</b></p> <p>Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982 (Vic).</p>	<p>The introduction of the DDL should not affect current processes for access and correction. However, Service Victoria and the DoT should ensure respective responsibilities are clear and that processes are built with a ‘no wrong door’ approach.</p> <p>See <a href="#">Section 5.1.3</a>.</p>
<p><b>IPP 7 – Unique identifiers</b></p> <p>A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.</p>	<p>Driver Licence numbers are unique identifiers in terms of the PDPA.</p> <p>Driver licence numbers will appear on the DDL. However, the DDL project does not involve the assignment of new unique identifiers.</p> <p>No issues identified.</p>

7. APPENDIX B – ASSESSMENT AGAINST THE IPPS

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DoT
<p><b>IPP 8 – Anonymity</b></p> <p>Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.</p>	<p>Not relevant for the DDL – identification is a required part of acquiring or using a DDL.</p>
<p><b>IPP 9 – Transborder data flows</b></p> <p>If an individual’s personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.</p>	<p>As far as IIS understands, the DDL processes are contained within Victoria.</p> <p>No issues identified.</p>
<p><b>IPP 10 – Sensitive information</b></p> <p>The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.</p>	<p>Driver licence processes do not involve the collection of sensitive information as defined, but do involve some biometric and health information (See <a href="#">Section 3.6.2</a>). Such information is part of the R&amp;L data that the DoT has already collected.</p> <p>No issues identified.</p>



Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

INFORMATION INTEGRITY SOLUTIONS PTY LTD

PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438

F: +61 2 9319 5754

E: [contact@iispartners.com](mailto:contact@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

ABN 78 107 611 898

ACN 107 611 898



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS



**Report: 19 June 2023**

**Department of Transport and Planning -  
Victoria**

**OFFICIAL: Sensitive**

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

# PRIVACY IMPACT ASSESSMENT - SERVICE VICTORIA DIGITAL DRIVER LICENCE PROJECT



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

## Contents

Glossary	1
1. Executive summary	1
1.1 IIS's overall view	2
1.2 Recommendations	3
2. Introduction	6
2.1 PIA scope	6
2.2 About this report	6
3. Project description	8
3.1 Background	8
3.2 Project objectives and scope	8
3.2.1 Objectives and expected benefits of the project	8
3.3 Project status	9
3.4 About the DDL	9
3.5 Participants in the DDL Project MVP	10
3.5.1 The Department of Transport and Planning	10
3.5.2 Service Victoria	11
3.5.3 Joint Venture Operator	11
3.5.4 Checkers— Victoria Police	11
3.5.5 Checkers – others, including pubs and clubs	12
3.5.6 Victorian citizens using a DDL	12
3.6 Nature of systems and information flows	12
3.6.1 Key system components	12
3.6.2 Kinds of information involved	13
3.6.3 Overview of information flows	14
3.7 Legal framework	19
3.7.1 Victorian laws	19

## CONTENTS

3.8	Project governance	20
4.	Approach to risk analysis	22
4.1	Inherent privacy risks	22
4.2	Positive privacy aspects	23
4.3	Residual privacy risk level	24
5.	Findings and recommendations	25
5.1	IPP issues or risks	25
5.1.1	Transparency – IPP 1 and IPP 5	25
5.1.2	Security – IPP 4	30
5.1.3	Access and correction – IPP 6, and privacy complaint handling	35
5.2	Governance	35
5.2.1	Project governance	35
5.2.2	Privacy by Design and future developments	36
6.	Appendix A – Methodology	38
6.1	PIA approach	38
6.2	Documents reviewed	38
6.3	Meetings held	39
7.	Appendix B – Assessment against the IPPs	40

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## Glossary

Abbreviation or term	Expansion or definition
(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
34(1)(b), 34(4)	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
IIS	IIS Partners and Information Integrity Solutions Pty Ltd
IPA	Information Protection Agreement
4(1)(b), 34	30(1), 34(1)(b), 34(4)(a)(ii)
IPP	Information Privacy Principle
JVO	The DTP's Joint Venture Operator for VicRoads
JWT	JavaScript Web Token
LOA	Level of Assurance
MVP	Minimum Viable Product
MMP	Minimum Marketable Product
OVIC	Office of the Victorian Information Commissioner
PDPA	<i>Privacy and Data Protection Act 2014</i>
PIA	Privacy Impact Assessment
QR Code	Quick Response Code
R&L	Registration & Licensing
The DTP	Department of Transport and Planning

0. GLOSSARY

Abbreviation or term	Expansion or definition
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VicPol	Victoria Police

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

# 1. Executive summary

The Department of Transport and Planning (the DTP) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. The DDL will be made available through the Service Victoria platform and app. A DDL will allow a licence holder to access an electronic version of their licence on a mobile device and present it in place of the physical licence.

The first phase of the Service Victoria DDL Project involved the production of a Minimum Viable Product (MVP) through the Service Victoria platform and testing via an internal pilot. The second phase is to test the minimum marketable product (MMP) via an external pilot starting with a regional pilot in Ballarat, which will commence in July 2023. 30(i), 34(1)(b), 34(4)(a)(ii)

The MMP would be a replication of the data and attributes from the existing Victorian driver licence to a digital credential through the Service Victoria digital wallet, with three primary use cases:

- Entitlement to drive
- Proof of identity
- the customer is over 18.

The DDL is one product being delivered in two channels; via Service Victoria and the Joint Venture Operator (JVO). The DTP through the JVO will share its driver licence data with Service Victoria. Due to the quantity and sensitivity of personal information that will be shared with and used by Service Victoria, the privacy impacts of the DDL Project need to be carefully examined. The DTP has previously engaged IIS Partners (IIS) to conduct a Privacy Impact Assessment (PIA) for the first phase of the SV DDL Project. This second PIA will assess the MMP for the regional pilot release and future full rollout. The scope of the PIA covers privacy risks associated with:

- Data flows between JVO and Service Victoria
- Security of the information
- Onboarding and user experience in the SV digital wallet
- Features and use cases within the MVP project scope
- Core privacy requirements under the Information Privacy Principles (IPPs).

In undertaking this PIA, IIS considered:

- Privacy principles in Victorian privacy law,
- Relevant legislation such as *Road Safety Act 1986* and the *Service Victoria Act 2018*
- Guidance materials published by the Office of the Victorian Information Commissioner (OVIC) and the Office of the Australian Information Commissioner (OAIC)
- Privacy good practice stemming from IIS's knowledge and experience.

## 1. EXECUTIVE SUMMARY

This report:

- Provides background to the project, including key project participants and roles, key systems and information flows, and the relevant legal framework.
- Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

The PIA methodology is included in the Appendices.

### 1.1 IIS's overall view

IIS has not identified any high-risk privacy issues for the project with respect to implementation of appropriate controls to manage the inherent high risks. Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. The issues identified arise in the context of the project stage, which is now turning to implementation and the full-roll out, and the complexity of the project environment.

30(1), 34(1)(b), 34(4)(a)(ii)

- There is significant quantity and sensitivity of personal information involved.
- The project will involve the display of Registration and Licensing (R&L) data in DDLs via individual's devices.
- The data involved includes sensitive biometrics, like driver images as well as R&L details.
- Both the JVO and Service Victoria are offering DDL apps, under the guidance of the DTP. The apps, while developed independently, are expected to meet the DTP's policy and design standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- Service Victoria's design has taken account of possible security risks for DDL users, Unacceptable risks from this modelling have been eliminated or are under management with a low risk tolerance.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including how checkers can interact with their devices, or handle personal information displayed via the DDL – can cause concern and jeopardise uptake of the solution.

## 1. EXECUTIVE SUMMARY

Overall, the DDL has benefited from being designed in a privacy-friendly way. Taking into account the positive privacy aspects such as the emphasis on data minimisation, the avoidance of a new digital footprint, the DDL security features, and expected detailed governance arrangements, we consider that the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, the development of privacy coordination and monitoring arrangements, and close attention to the possible security risks for customers using a DDL.


IIS has identified the following key privacy risks and issues for consideration at this point in the project:

- **Transparency and privacy complaint handling**
  - Public communications have been developed and should provide a good basis for public awareness about DDL and privacy and security approaches. However, in some areas the current messages lack detail or might be over-reassuring. Additional information activities are planned but not yet finalised – they will need to address a range of issues to ensure the risks as well as positives of using a DDL are known.
- **Security**
  - If not already, privacy risks for individuals should be included in project privacy risk registers and monitored.
  - Rules and instructions around handling of individuals devices for DDL checking should be in place.
- **Privacy governance**
  - As more detailed arrangements for ongoing project governance are settled, they need to ensure there are clear privacy roles and responsibilities, including for monitoring privacy outcomes.
  - Continuing the use of privacy by design will be important as the DDL project proceeds.

### 1.2 Recommendations




IIS makes nine recommendations for the SV DDL project. For each recommendation, we have suggested who would be responsible for carrying out the recommendation (the DTP, Service Victoria, or both) and the timeframe for completion. We have specifically highlighted the recommendations that in our view must be completed before the pilot against those that should be completed within the next six months before full rollout or to be carried as an ongoing risk treatment

Legend:

IIS recommended priority to undertake risk treatment	Symbol
Before pilot	



1. EXECUTIVE SUMMARY

Recommendations	Who	Timeframe
<b>Recommendation 1</b> – Ensure that project agreements and governance arrangements provide for a process for ensuring that privacy messages are consistent and adopt best privacy practice.	Service Victoria, JVO & DTP	For full rollout
<b>Recommendation 2</b> – Service Victoria privacy policy to include comprehensive DDL information.	Service Victoria	For full rollout
<b>Recommendation 3</b> – Ensure DDL privacy and security information is accurate and does not overstate benefits	Service Victoria, JVO & DTP	For pilot and ongoing 
<b>Recommendation 4</b> – Include privacy 'satisfaction' in the evaluation of pilot communications.	Service Victoria & DTP	For pilot 
<b>Recommendation 5</b> – Continue to monitor, assess and update privacy risks in risk register.	Service Victoria & DTP	For pilot and ongoing 
<b>Recommendation 6</b> – Explore options for limiting address display on the DDL driver licence view.	Service Victoria & JVO	For full rollout
<b>Recommendation 7</b> – Document and communicate requirements for the handling of individuals devices for DDL checking.	DTP	For full rollout
<b>Recommendation 8</b> – Ensure project governance arrangements include clear privacy roles and responsibilities, including for monitoring privacy outcomes.	Service Victoria & DTP	For full rollout

## 1. EXECUTIVE SUMMARY

Recommendations	Who	Timeframe
<b>Recommendation 9</b> – Continue to adopt privacy by design in the DDL’s further development.	Service Victoria & DTP	Ongoing

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## 2. Introduction

The DTP and Service Victoria are working to bring digital driver licences to Victorian residents, to be made available through the Service Victoria platform. The DTP engaged IIS to conduct a PIA on the minimum marketable product (MMP) of the SV DDL for the planned regional pilot release and future full rollout. This is the second PIA that IIS has conducted on this project – the first MVP PIA was completed in June 2022.

### 2.1 PIA scope

Service Victoria is responsible for the design of the DDL, in accordance with the DTP's specified standards. DTP is also the data owner of R&L data and will provide the data 30(1), 34(1)(b), 34(4)(a)(ii) 30(1), 34(1)(b), 34(4)(a)(ii) to populate the DDL. The PIA will entail end-to-end consideration of privacy issues that could have an operational impact from the perspective of the DTP, JVO and Service Victoria.

The first phase of the project involved the development of a MVP. This phase of the project is to test the DDL by conducting an initial regional pilot in Ballarat, potentially conduct more pilots and looking towards full public rollout by 2024. The purpose of this PIA is to identify any privacy issues that might arise from the project's design and initial implementation approaches, and to make recommendations to address the potential issues.

In providing this report, IIS makes the following qualifications:

- The PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features
- The PIA is based on information gathered from, and provided by, the DTP, JVO and SV
- IIS does not provide legal advice; rather we provide strategic privacy and cyber security advice.

### 2.2 About this report

The report is structured to provide an overview of the DDL project, explain IIS's approach to risk analysis, analyse privacy issues according to the project scope, and provide additional context to the PIA work:

- **Project description** ([Section 3](#))  
Provides background to the DDL Project, key project participants and roles, key systems and information flows, and the relevant legal framework.
- **Approach to risk analysis** ([Section 4](#))  
Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.

- **Findings and recommendations** ([Section 5](#))

Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

- **Appendix A – Methodology** ([Section 6](#))

Summarises our methodology, including list of documents reviewed and meetings held.

- **Appendix B – High-level assessment against the IPPs** ([Section 7](#))

Provides a high-level assessment of the DDL project against the IPPs and notes risks areas, which are discussed in detail in [Section 5](#).

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## 3. Project description

### 3.1 Background

Service Victoria and the DTP are working to bring DDLs to Victorian residents. Three out of six Australian state and territory jurisdictions have either trialled or have a legislation-based DDL. Service Victoria has identified that there are 4.6 million active Victorian customers who use the Service Victoria mobile application, and over 4 million Victorians possess a driver licence. Service Victoria has been progressing delivery of the DDL in collaboration with the DTP.

The DDL will replicate data and attributes from an existing plastic Victorian driver licence to a digital credential. The DDL will have three primary use cases:

- Entitlement to drive whilst on the road
- Proof of identity
- Casual proof of age and photo for licenced venues and businesses such as supermarkets, convenient stores, tobacco retailers, etc.

The DDL products will support verification and, for Service Victoria sharing of the information, presented on various DDL views using QR code scanning. This feature will enable individual and business customers to validate the details presented by a DDL holder without requiring specialised hardware or facial recognition.

The project is currently working towards a first release, commencing with an external pilot. At this stage, the DDL will be supplementary to the physical driver licence and will not replace it. While most full licence drivers do not need to carry a physical licence, where the existing laws do require this, they remain enforceable. For example, the introduction of DDLs does not change the obligation of motorists such as learner and probationary drivers to carry their physical licence with them at all times.

### 3.2 Project objectives and scope

#### 3.2.1 Objectives and expected benefits of the project

The DDL is consistent with the Victorian Government's digital strategy, which is expected to deliver cost savings, and better, fairer, and more accessible services, and a digital ready economy.

The expected benefits of the DDL for Victorian drivers are:<sup>1</sup>

- Freedom – After the pilots, most customers will be able to leave their physical licence and wallet at home.
- Peace of mind – Customers know their DDL is always on their phone as a backup.

---

<sup>1</sup> See the 050522.DDL.Pilot.Scope.UC.Roadmap.

- Convenience – 89% of the consulted customers indicated that they believe the DDL to be more convenient than a physical driver licence because they always carry their phone with them.
- Security – Customer’s personal information is protected and only accessible via user login, or 6-digit PIN.
- Privacy – Information sharing can only be initiated by the customer, and the intention is that where circumstances permit, customers will be able to limit the amount of information exchanged.
- Up-to-date data management – Customers using a DDL have access to up-to-date information about the status of their licence; whether it is valid or has expired.

### 3.3 Project status

Service Victoria and the DTP are taking an iterative approach to the DDL project. Service Victoria and the DTP have undertaken significant development work since the initial MVP in 2022. The design and build of the Service Victoria DDL are complete. Formal agreements and approval on matters including final design, security and governance are currently underway. SV and DTP are now in the testing and roll out phase for the DDL.

In regard to pilots, one internal pilot was completed and a regional external pilot is planned for July 2023:

- Internal pilot was completed to test the DDL end-to-end journey, including identity verification, adding the DDL to the Service Victoria’s Digital Wallet and the communication between Service Victoria and the DTP systems. This is only for full-licence car drivers, and without the QR Code. The DTP did not transfer ‘real’ data to Service Victoria for this pilot.
- Regional external pilot expected in July 2023 which will place in Ballarat with a focus on motorcycle, heavy and light vehicles for full licences holders above 21 years old. The external pilot will test matters including the use of the QR code verification by local business and authorities such as Victoria Police (VicPol). As noted, at the MMP stage, drivers will still need to carry their plastic licence. Demerit points is not in the scope of this pilot.

At the time of writing this report, IIS was not aware of any further planned regional pilots but note that there could potentially be more.

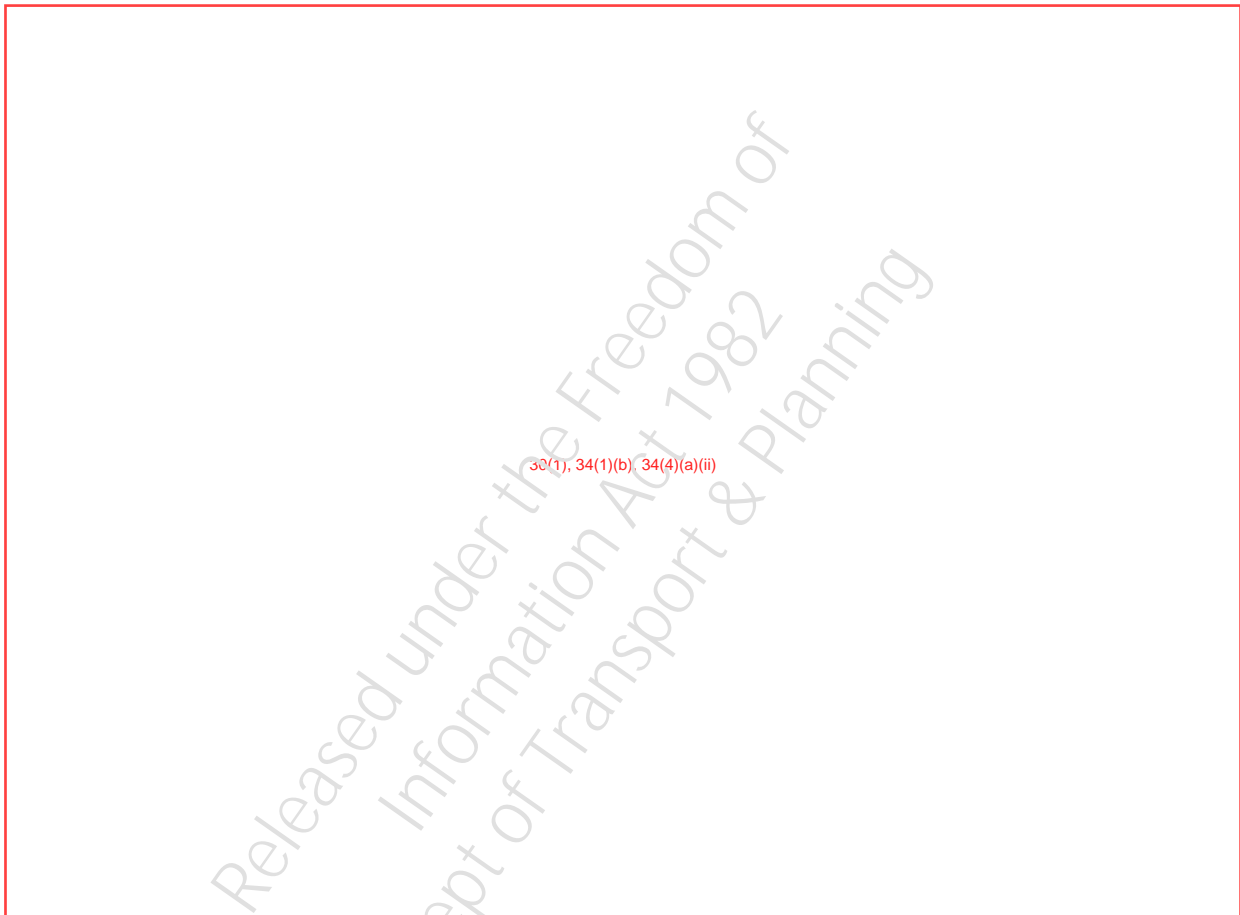
### 3.4 About the DDL

The DDL will be accessible through the customer’s Service Victoria’s digital wallet in the Service Victoria app. The app supports selective disclosure, which means the holder has the ability to show and verify subsets of their DDL details – for example, only revealing the fact they’re over 18, rather than sharing their exact birthdate, driver licence number, address and other information, as they would be forced to do with a physical licence. These details are verified by a QR code that will be scanned by checkers to verify the licence status.

The DDL will contain features, such as holograms, manual refresh, display of the last refreshed date and time and a watermark, that are digitally equivalent to the features that indicate a plastic licence is legitimate.

DDLs will also have additional security features:

- DDLs are protected by the user's phone password (if used) and is only accessible by logging into the SV app via a user login, biometric identification, or six-digit PIN.



Law enforcement checkers will have an authority app to check the barcode on the DDL (similar to the ones on the physical driver licence). Non-law enforcement checkers will be able to scan the QR code via the QR Code reader from the regular, publicly distributed SV app.

### **3.5 Participants in the DDL Project MVP**

This section sets out the participants in the DDL project.

#### **3.5.1 The Department of Transport and Planning**

The DTP operates and coordinates Victoria's transport network, the delivery and upgrade of transport infrastructure, as well as the reforms to road safety policy, regulatory and legislative environment. The DTP will remain the owner of the R&L data.

The DTP is also the policy owner of driver licensing policy. All the elements that relate to licence information, entitlement to drive, safety and roads will stay with the DTP. The user's licence features and potential changes (e.g., addition of a licence, expiration, suspension) are managed on the DTP's side, and SV only reflects those changes through the DDL.

### 3.5.2 Service Victoria

Service Victoria was created by the Victorian Government to modernise Victorian customer's online government services and make it easier for people to complete more online services more often from the comfort and safety of their own homes. Customers can access more than 80 government services through SV

Service Victoria is responsible for the solution delivery through the Service Victoria app (as one of two channels), as the JVO will also deliver its own version through its forthcoming myVicRoads app. Service Victoria is in charge of the maintenance of the app and ensuring that the right security, privacy and compliance features are in place. Service Victoria is also responsible for the communications with customers and will provide a digital channel for customer feedback about the DDL via a feedback on the app to ask for customer feedback regarding the add of the DDL to the Service Victoria wallet. Customers can provide both quantitative and qualitative feedback.

Over time, the Service Victoria digital wallet is expected to include a wide range of Victorian government licences and permits.

### 3.5.3 Joint Venture Operator

The JVO is responsible for customer service in relation to R&L and operational activities (except in relation to complex customers), initial level of customer complaint, and management of the DTP's IT systems. [redacted] 30(1), 34(1)(b), 34(4)(a)(ii)

[redacted] 30(1), 34(1)(b), 34(4)(a)(ii) Additionally, the JVO is providing and operationally supporting the APIs required to integrate with Service Victoria.

The JVO is also responsible to producing a DDL in its app.

### 3.5.4 Checkers – Victoria Police

VicPol is a key stakeholder for the DDL and is working with DTP to identify and resolve any issues.

The external regional pilot will be used to test the efficacy of, and seek feedback on, the VicPol app already available to check the barcode, which IIS understands contains only the licence number. VicPol will only be checking the DDL as an initial check. It will continue to verify the physical driver licence

[redacted] 30(1), 34(1)(b), 34(4)(a)(ii) The pilot will help identify any needed modifications of police processes if/when the DDL is a legally binding driver licence, or if the program adopts ISO 18013-5 mDL interoperability standards in Victoria, giving VicPol the ability to scan driver licences from any state or territory.



### 3.5.5 Checkers – others, including pubs and clubs

For the external pilot, a number of businesses that need to validate licences or identification will be selected in Ballarat, these will include:

- National Retailers Licensed venues such as bars, pubs, nightclubs and restaurants
- Hotels
- Petrol service stations
- Supermarkets and grocery stores
- Convenience stores
- Tobacco retailers
- Licensed premises, parcel pickup and delivery businesses, retailers offering click and collect, credit options and equipment hire.

IIS notes that the initial focus will be on small businesses that do not need to retain documentary evidence of identity. Such requirements might be considered in further iterations of the DDL.

### 3.5.6 Victorian citizens using a DDL

The external pilot will take place in the regional centre of Ballarat, only for drivers with a full licence including car, motorcycle, light, heavy vehicles. Service Victoria estimates a maximum of 5,000 customers for the pilot.

After the pilot, the DTP expects the DDL will be extended to all licence holders including probationary drivers and learner drivers in further stages of the project.

## 3.6 Nature of systems and information flows

### 3.6.1 Key system components

#### 3.6.1.1 The DTP

The main DTP systems involved for the DDL are:

- 
- 

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

### 3.6.1.2 The JVO

30(1), 34(1)(b), 34(4)(a)(ii)

, 34(1)(b), 34(4)(i) The APIs will allow b(1), 34(1)(b), 34(4)(a)(i) driver licence data to be retrieved by the front-end mobile apps developed by the JVO and Service Victoria.

### 3.6.1.3 Service Victoria

To build the DDL, Service Victoria is reusing existing infrastructure previously used within Service Victoria. An advantage here is that Service Victoria has confidence in the systems, including because a number of components have already gone through security audits.

The Service Victoria platform hosts the app. The customer must download the app on their device and create an Service Victoria account to be able to generate a DDL and hold it within their digital wallet.

### 3.6.1.4 Licence holders

Licence holders will use their own devices to set up, or use, an Service Victoria account, and to add a DDL to the Service Victoria digital wallet within the mobile app.

## 3.6.2 Kinds of information involved

### 3.6.2.1 Personal information

The kinds of personal information to be shared by the DTP is the same as what currently appears on the plastic licence. This is:

- Full name
- Date of birth
- Full address
- Signature
- Photo
- License number
- License expiry date
- Licence type (car/bike/dual)

- Licence proficiency (full/probationary)
- Licence category (heavy vehicle categories)
- Licence conditions
- Card Number
- Issue Date
- Licence Status.

The DDL QR Code will also display information which will vary depending on the customer's preferences. The aim is that more sensitive licence information will only be available under the photo of the licence when a user opts to display their full licence.

The DTP will also share information that will allow the following information to be displayed via the QR Code:

- Show the customer's full driver licence details (including status)
- Prove the customer's identity.
- Prove the customer is over 18.

### 3.6.2.2 Sensitive information and health information

The DTP will also share some limited medical information about licence holders. This is in the form of conditions included on driver licences (e.g., use of glasses when driving). IIS considers the codes that are associated with a medical condition meet the definition of health information.

The DTP will also share biometric information with Service Victoria in the form of the licence photo and signature. Biometric information is not explicitly contained in the definition of sensitive information in the *Privacy and Data Protection Act 2014*. However, it is considered sensitive information under the *Privacy Act 1988* (Cth) and OVIC advises organisations to consider treating biometric information as 'delicate information' and to handle it cautiously.<sup>2,3</sup>

### 3.6.3 Overview of information flows

At a high level, the arrangements for the DDL are expected to involve the following:

- 

30(1), 34(1)(b), 34(4)(a)(ii)

<sup>2</sup> Please refer to the definition given by OVIC: "Delicate information' refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regard as requiring a higher degree of protection.", available at [https://ovic.vic.gov.au/book/key-concepts/#Sensitive\\_and\\_delicate\\_information](https://ovic.vic.gov.au/book/key-concepts/#Sensitive_and_delicate_information).

<sup>3</sup> See <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>.

- As noted, Service Victoria will be using its existing infrastructure and processes for Service Victoria accounts and digital wallet to support the DDL. It will add a QR code generation process. Customers will use an existing Service Victoria account, or set one up, requiring consent-based identity verification (at a level of assurance two in accordance with its Identity Verification Standards).<sup>4</sup> Service Victoria is designing its system to allow for secure 'blind' pass through of data between the DTP to a customer's device. It will 'see' personal information only at the QR code generation step and will not retain any personal information, including in audit logs.
- Customers can choose to show their DDLs to checkers (law enforcement agencies, or businesses seeking proof of identity or age).

The following section describes in more detail the information flows relating to the creation of a Service Victoria account and the creation of a DDL in the Service Victoria app. It also describes the information flows when a QR Code is generated and validated using the Service Victoria app (both by the customer and the checker).

Steps for the user	Back-end processes
Log into the app / create an account	
<p>The customer logs into the app.</p> <p>If the customer doesn't have an account, they create one and start by entering the email address, password, first and second name in required fields. The customer creates a six-digit PIN and can set up biometric authentication (such as their face or fingerprint).</p>	<p>If an account is created, email address and mobile phone (if provided) are verified via the use of a one-time password.</p>
Add the DDL to the wallet	
<p>In the 'My Wallet' tab of the app, there will be an 'Add Driver Licence' button. The customer taps on this.</p> <p>At this point the customer provides their consent to verify their ID documents and Australian driver licence.</p>	<p>This will trigger the normal flow in the back end for when there has been a request to add something to the wallet.</p> <div style="border: 1px solid red; padding: 5px; text-align: center; color: red;">                     30(1), 34(1)(b), 34(4)(a)(ii)                 </div>

<sup>4</sup> See <https://service.vic.gov.au/about-us/service-victoria-identity-verification-standards>.

Steps for the user	Back-end processes
Verify identity with choice of ID	
<p>The customer provides consent to verify their identity at a level of assurance two (LOA2). This requires the customer to provide two satisfactory identity documents from the list below:</p> <ul style="list-style-type: none"> <li>● a full Australian birth certificate; OR</li> <li>● a full Australian passport; OR</li> <li>● a foreign passport with a valid Australian visa; OR</li> <li>● an ImmiCard; OR</li> <li>● an Australian Citizenship Certificate; OR</li> <li>● an Australian driver licence; OR</li> <li>● a Medicare card.</li> </ul>	<p>The customer undergoes identity verification. <span style="border: 1px solid red; padding: 2px;">(1)(b), 34</span></p> <div style="border: 1px solid red; height: 150px; width: 100%; display: flex; align-items: center; justify-content: center;"> <span style="color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</span> </div>
<p>The user is presented with the choice to create an ongoing Electronic Identity Credential that will be valid for 10 years.</p> <p>If the user has an account with an existing electronic identity credential (EIC) at Level of Assurance (LOA2) or above, Service Victoria validates the identity.</p>	<p>If the customer consents to creating an ongoing Electronic Identity Credential, <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span></p> <div style="border: 1px solid red; height: 100px; width: 100%; display: flex; align-items: center; justify-content: center;"> <span style="color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</span> </div>
Verification of driver license details (in order to access DDL)	
<p>The customer is presented with a screen requiring them to enter the following information:</p> <ul style="list-style-type: none"> <li>● Name (as it appears on their physical driver licence)</li> <li>● License number</li> <li>● License expiry</li> <li>● Unique card number (optional)</li> </ul>	<div style="border: 1px solid red; height: 200px; width: 100%; display: flex; align-items: center; justify-content: center;"> <span style="color: red;">30(1), 34(1)(b), 34(4)(a)(ii)</span> </div>

Steps for the user	Back-end processes
	<p>30(1), 34(1)(b), 34(4)(a)(ii)</p>
Loading DDL	
	<p>Upon verification, the personal information (including the image of the individual) is encrypted</p> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> <p>As soon as the DDL is added to the wallet, the name data is deleted from Service Victoria's platform.</p>
The customer can now access the DDL from the Service Victoria wallet.	<p>30(1), 34(1)(b), 34(4)(a)(ii)</p>

Released under the Freedom of Information Act 1982  
Dept of Transport & Planning

Steps for the user	Back-end processes
QR Code generation and validation	
<p><b>Generating a QR Code:</b></p> <p>The user will be given the choice to decide on different sharing options. This will allow them to determine how much of their driver licence information they'd like to show to non-law enforcement checkers.</p>	<p>30(1), 34(1)(b), 34(4)(a)(ii)</p> <p>The QR code that is generated is only valid for two minutes before it refreshes and the encrypted data on the platform is deleted at the same time.</p>
<p><b>Validating a QR Code:</b></p> <p>Law enforcement and businesses that require proof of age or proof of eligibility to drive will be able to scan the QR code to verify its validity and to see the licence information (what is shown will depend on the policy about differential display, and then on what the DDL user chooses to display).</p>	<p>30(1), 34(1)(b), 34(4)(a)(ii)</p>

## 3.7 Legal framework

### 3.7.1 Victorian laws

The DDL project must comply with the following relevant laws.

#### 3.7.1.1 Privacy and Data Protection Act 2014

The *Privacy and Data Protection Act 2014* (PDPA) regulates the handling and protection of personal information by Victorian public sector organisations. Organisations subject to the PDPA must comply with the Information Privacy Principles (IPPs) that contain requirements across the information lifecycle. Part 4 of the PDPA gives the Victorian Information Commissioner the power to prescribe security requirements pertaining to public sector information and information systems through the Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS).

#### 3.7.1.2 Health Records Act 2001

The *Health Records Act 2001* (HRA) and its Health Privacy Principles (HiPPs) regulate the collection, handling and protection of health information, which includes information or opinion about the physical or mental health or disability of an individual.<sup>5</sup>

#### 3.7.1.3 Road Safety Act 1986

The *Road Safety Act 1986* (RSA) is the main piece of legislation that regulates the use of roads, registration of vehicles and driver licensing in Victoria.

The DTP and Service Victoria have had a Service Agreement since 2017. For the DTP to disclose the data to Service Victoria, the DTP and Service Victoria also had to enter into an Information Protection Agreement (IPA) in accordance with section 90N of the RSA. No legislative changes to the RSA are needed for the MMP, as the recent amendments of the RSA and the *Service Victoria Act 2018* are sufficient to deliver the pilot. In the longer term, changes to RSA might be necessary to incorporate digital services.

Part 7B of the RSA applies to Service Victoria because it has requested access to the driver licence information held by the DTP where the information may identify an individual or allow an individual's identity to be ascertained. Part 7B contains the protective framework for relevant information, including the allowed purposes for use and disclosure of relevant information, the exceptional circumstances for the use and disclosure of relevant information, the uses of relevant information for verification purposes, etc.

---

<sup>5</sup> The HPPs are substantially similar to the IPPs. For the purposes of our privacy analysis in Section 5, IIS has focused on the IPPs.



#### 3.7.1.4 Service Victoria Act 2018

The *Service Victoria Act 2018* provides for the delivery of government services to the public by Service Victoria and provides a regulatory framework for the provision of identity verification functions by the Service Victoria CEO. Importantly, the Act establishes that the Service Victoria CEO must comply with identity verification standards when verifying identity. These standards are set out separately to the legislation and provide a consistent and secure identity verification framework for people transacting with the Victorian Government through Service Victoria. Among other things, the *Service Victoria Amendment Act 2022* added new provisions supporting digital delivery of Victorian licences.

#### 3.7.1.5 Charter of Human Rights and Responsibilities Act 2006

The *Charter of Human Rights and Responsibilities Act 2006* (the Charter) is a Victorian law that sets out the protected rights of all people in Victoria as well as the corresponding obligations on the Victorian Government. The DTP will be conducting a Charter assessment with particular focus on engagement or limitation of the right to privacy.

#### 3.7.1.6 Road Safety (Drivers) Regulations 2019

Regulation 63 of the Road Safety (Drivers) Regulations 2019 describes the details that driver licence or learner permit documents must contain, including the identification number, the person's first name, second and third initials (if any) and family name; a photograph of the person; the person's residential address; the person's date of birth; a reproduction of the person's signature; the category or categories of driver licence; its expiry date; and the code of any condition to which the licence or permit is subject.

### 3.8 Project governance

In November 2021, the Interdepartmental Committee (IDC) endorsed preliminary detailed scoping work to support an MVP release strategy.

At project initiation, Service Victoria provided the DTP with an initial delivery agreement. This agreement specified the scope and timeline for work. IIS understands that the authorising structure for the project has now changed. Policy governance matters sits with the DTP and Service Victoria is one of the delivery channels.

As the project has continued to progress, several governance arrangements that have been put in place includes:

- Ministerial oversight via monthly ministerial meetings
- Steering committee with senior staff from Service Victoria and the DTP
- Working groups sitting under the steering committee with weekly meetings
- Development of DDL standards set by the DTP which include the DDL Policy Standards and the DDL design standards.

These arrangements are now moving to a more formal partnership arrangement with the DTP, taking account of the fact that the authorising governance will be coming from Cabinet, as well as the JVO, which will see modernisation of its systems and processes.

The arrangements include:

- Ministerial oversight
- A Memorandum of Understanding (MoU) between Service Victoria and the DTP, setting out overall principles on how the relationship works and a high-level governance framework
- Operating service commitment
- Transaction journey documents
- Information Protection Agreement.

These documents and processes set expectations and respective roles and responsibilities, including with respect to privacy.

IIS understands the MoU remains in effect and that the iPA is currently being updated. Service Victoria and the DTP are working through further governance arrangements and relevant documents including a Communications Plan and the updating of privacy documents. These will need to be finalised before the DTP provides R&L data to Service Victoria for the DDL. IIS also understands that the structure of project steering committee and related working groups and consultative processes will continue.

## 4. Approach to risk analysis

In undertaking this PIA, IIS considered:

- The IPPs in the PDPA
- Guidance materials published by the OVIC and the OAIC
- Privacy good practice stemming from IIS's knowledge and experience.

The PIA focuses on privacy risks that are introduced or heightened by the DDL Project, rather than privacy risks for existing processes to issue and use driver licences.

This section assesses the project's residual privacy risk level, by weighing the inherent privacy risks against the existing privacy positive aspects.

The following section discusses the project's privacy issues and risks identified in detail and makes recommendations to mitigate the risks.

### 4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks. Inherent privacy risks arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential (including value) for, and consequences of, misuse
- The range of people from whom the information may be collected
- The context in which personal information is handled – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the project
- The extent to which information is accessed or handled by third parties
- The likely community and/or media interest in the privacy aspects of the project.

Taking account of these factors, IIS considers the DDL project

30(1), 34(1)(b), 34(4)(a)(ii)

1), 34(1)(b), 34(4)(a)

- There is significant quantity and sensitivity of personal information involved.
- The project will involve the display of Registration and Licensing (R&L) data in DDLs via individual's devices.
- The data involved includes driver images as well as R&L details.
- Both the JVO and Service Victoria are offering DDL apps, under the guidance of the DTP. The apps, while developed independently, are expected to meet the DTP's policy and design standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.

- Service Victoria's design has taken account of possible security risks for DDL users. However, DTP is currently conducting further security assessment processes. IIS notes these would be concluded before the project proceeds for the regional pilot.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including how checkers can interact with their devices, or handle personal information displayed via the DDL – can cause concern and jeopardise uptake of the solution.

## 4.2 Positive privacy aspects

IIS considers that the DDL Project has important positive aspects that support privacy and minimise the inherent risks associated with the project. These are outlined below:

### Positive privacy aspects with the project/solution design

- Service Victoria has followed the key privacy enhancing strategy of data minimisation – it will handle minimal personal information and will not retain any such information. In particular:
  - When the DDL has been added to the Service Victoria wallet, the only thing stored in Service Victoria's platform is a linking key 34(1)(b), 34(1)(c) in the wallet database. This indicates that the user has a driver licence in their wallet, and the platform uses that linking ID to get the driver licence information from the DTP.
  - The path through Service Victoria's platform from the DTP to the app is automated; no licence information is stored, and no Service Victoria personnel will have access to it as it passes through the platform. Service Victoria specified that there are no 'dead letter queues' or any other place where information may inadvertently be stored.
- The DDL project design appears to avoid the risk of a new digital footprint, in that neither Service Victoria or the DTP will have any detailed records that would enable them to track when, or to whom, a customer presents their DDL for checking. The DTP will keep an audit log, which would allow it to identify and investigate a transaction.
- The DDL does not rely on the creation of duplicate stores of personal information. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) This means the DTP data remains the single 'source of truth' for driver licence information.
- The device used to display the DDL only holds the image of the licence. The information embedded in the QR code is information that have been validated by Service Victoria and is only available for display without refresh for a limited period of two minutes.

### Governance and risk management

- Service Victoria and DTP have indicated a commitment to privacy and appear to have this in mind as the project design is finalised and as it progresses to implementation, this includes having appropriate governance arrangements in place to support privacy requirements.

- The arrangement between the DTP and Service Victoria is governed by an MoU and IPA (as required under Part 7B of the RSA). These documents contain the roles and responsibilities of both parties and in particular the privacy and security obligations.
- Service Victoria has undertaken considerable consultation and design work in collaboration with the DTP. Its future directions are now subject to formal agreement and approval on matters including final design, security and governance, and on the outcome of two planned pilots.
- The DTP has liaised with Service Victoria to assess its security culture and risk management in the context of the DDL.
- Service Victoria's design has taken account of possible security risks for DDL users. Service Victoria 30(1), 34(1)(b), 34(4)(a)(ii) to perform a well architected framework review of the solution and has had two independent penetration tests conducted against the build.
- DTP has completed an Information Value Assessment incorporating feedback from Service Victoria's own Information Value Assessment.
- DTP has conducted independent security assessment processes.

#### Privacy advantages for DDL users over the existing plastic driver licence

- The DDL is potentially more secure in that it is protected by device and Service Victoria app security measures, including password or PIN protection.
- The DDL includes a range of other security features and further work is being undertaken to identify if other measures are needed.
- If a DDL is reported stolen or lost and has been cancelled by the DTP, this will be reflected in the DDL and the QR code will not be able to be refreshed and verified.
- A customer's DDL can be validated in real-time. This means data can be instantly verified by scanning the QR code displayed on the DDL within the Service Victoria app.
- DDL users will have some choice about what information they display to checkers.

### 4.3 Residual privacy risk level

Overall, the DDL is likely to benefit individuals and it is being designed with privacy and trustworthiness as key considerations. Rather, the issues identified arise in the context of the project stage and the complexity of the project environment.

In summary, with a number of important issues to resolve, IIS considers the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, the development of privacy coordination and monitoring arrangements, and close attention to the possible security risks for customers using a DDL.

## 5. Findings and recommendations

This section discusses relevant privacy risks and issues that IIS has identified during the PIA.

The recommendations focus on mitigating privacy risks and improving practice during the further development of the DDL. For each recommendation, we have suggested who would be responsible for carrying out the recommendation (the DTP or Service Victoria, or both).

### 5.1 IPP issues or risks

A high-level analysis of the DDL project against the IPPs is at [Appendix B](#). IIS considers that the DDL project would be mostly consistent with the IPPs. For example:

- The project operates within the existing legal framework.
- Service Victoria will be authorised to collect and handle limited, generally encrypted, personal information consistent with the Service Victoria Act 2018.
- Anonymity is not practicable.
- The project will operate within Victorian borders.

The main IPPs where IIS has identified issues are in relation to openness, security, access and correction, and privacy complaint handling.

#### 5.1.1 Transparency – IPP 1 and IPP 5

Transparency provisions in the IPPs aim to allow individuals to make informed choices about providing information or using a service and to have a general understanding of how information about them is being handled. Transparency is both a matter of compliance as well as key to building public confidence and trust in the DDL. The IPPs provide two transparency mechanisms:

- Specified details provided at the point personal information is collected (IPP 1.3)
- General information available about the type of personal information agencies collect and hold and how it is managed (IPP 5.1).

##### 5.1.1.1 Privacy collection notice and privacy policy

At the time of writing this PIA, IIS understands that both the DTP and Service Victoria are undertaking work on their privacy collection notices and privacy policies.

In regard to the collection notice, IIS notes that Section 12.1 of the MoU states that collection notices will be provided by the DTP. IIS has been informed that a layered approach to the notices will apply:

- Service Victoria's collection notice will refer to the collection of data necessary to add a DDL within the Service Victoria app
- The DTP's collection notice will refer to the collection and use of R&L information.

Service Victoria shared with IIS a draft collection notice for the DDL internal pilot. IIS found the collection notice to be clear; we did not identify any issues in term of the requirements of IPP 1.3. We note that the same collection notice will be used for the regional pilot.

IIS understands Service Victoria will continue to develop its privacy materials in consultation with DTP, and following the established Service Victoria style guide and pattern (in accordance with the MoU). IIS notes that the DTP is inclined to follow Service Victoria's approach and will ensure that the JVO aligns with such approach.

Noting that both the DTP and Service Victoria are working on privacy materials, it is important that there is a clear process for coordinating and approving the privacy materials across the DDL project. We also understand that the DTP policy intent is that the privacy information for the myVicRoads and Service Victoria apps will be consistent.

**Recommendation 1 – Ensure that project agreements and governance arrangements provide for a process for ensuring that privacy messages are consistent and adopt best privacy practice.**

Establish project agreements and governance arrangements to ensure that privacy messages delivered by the DTP, JVO and Service Victoria are consistent, comprehensive and adopt best practices approaches.

**Who:** Both Service Victoria and DTP

**Timeframe:** For full rollout and ongoing

IIS considers that Service Victoria would need to have privacy information about the Service Victoria account, app, and the Service Victoria DDL on its website and also at relevant places in the app. It will be particularly important that the DDL app makes clear what personal information will be shared when an individual presents their phone to a checker. IIS also considers the more general communications for the pilot should address the question of DDL processes where a venue would currently take a copy of a plastic licence. For example, it might be that customers would be encouraged to offer both the DDL and the plastic licence in these circumstances.

In relation to Service Victoria's privacy policy, IIS encourages Service Victoria to include an D(1), 34(1)(b), 34(4)(a)(i) 30(1), 34(1)(b), 34(4)(a)(ii) on the information handling for DDLs for the full public rollout (noting that the Ballarat trial will be relatively small and involve low numbers) just as it has done so for the COVID-19 digital certificate. This might cover, for example, information about:

- Collection and handling of information for identity verification
- Activity logs
- Data security, including steps to take if a device is lost or stolen

- QR Codes, including what they contain and how they are refreshed
- Licence or credential checker handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

### Recommendation 2 – Service Victoria privacy policy to include comprehensive DDL information.

Include comprehensive DDL information for the full public rollout in Service Victoria's privacy policy.

Include an additional 30(1), 34(1)(b), 34(4)(a)(ii) section on the information handling for DDLs, which should cover matters such as:

- Collection and handling of information for identity verification
- Activity logs
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential checker handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

**Who:** Service Victoria

**Timeframe:** For full rollout

#### 5.1.1.2 Public communications and education

In addition to the specific requirements in the IPPs, active public awareness and education for DDL users and checkers will support transparency about the project, and support individuals' ability to exercise their privacy rights and to use a DDL safely.

IIS notes that Service Victoria, the DTP and the JVO have collaboratively developed a Communications and Engagement Plan<sup>6</sup> (the C&E Plan) which IIS has reviewed. The C&E includes the narratives and key messages for the regional pilot as well as communications and engagements tactics and timings in preparation for the full rollout. The narratives and key messages provide a good high-level overview of the solutions offered by both Service Victoria and the JVO.

The Communications Team is also working on a number of collaterals to promote public awareness and educations which include FAQs, Factsheets, an instructional video for users as well as briefing packs. IIS considers these efforts to be important in not only driving uptake but to ensure that Victorians are adequately informed about the DDL and its processes.

<sup>6</sup> Communications and Engagement Plan April 2023.



Additionally, IIS considers it is important that the public communications also include the following:

- The difference in approach between the DDL via Service Victoria and JVO.
- Clear information about how to use the DDL and validate a DDL, explicitly informing users and checkers that the licence image on the Service Victoria wallet is simply a replicated image and that the verified licence details are encrypted within the QR Code.
- Adequate information on what sharing options are available for the DDL, how to generate the QR Code, what the process is when allowing checkers to sight a DDL user's QR code and what their rights are.
- Develop security advice for customers, which is updated as any threats emerge. IIS considers that it is important the benefits are not overstated, given existing risks of fraud, misuse, or data breach.
- Make clear to customers that DDLs might not be accepted in all circumstances at least initially, including overseas. For example, validators might not take up the QR code scanning option, or they need to take a copy of a licence. While it might be OK to 'leave your plastic in your pocket', it might be clearer to encourage customers to have the plastic card with them during the pilot period.<sup>7</sup> In addition, while IIS understands that customers do not need to have a licence with them, except where there is a legal requirement to carry, e.g. learners and probationary drivers, it might be helpful to make this clear.

---

<sup>7</sup> <https://www.vicroads.vic.gov.au/licences/digital-driver-licence/register> viewed 11 June 2023

### Recommendation 3 – Ensure DDL privacy and security information is accurate and does not overstate benefits.

Ensure that communication for the DDL:

- Provide clear information about the differences between the JVO and the Service Victoria apps, in particular what information is shared with validators and whether or not an Internet connection is needed.
- Provide clear information about how to use the DDL and validate a DDL.
- Do not overstate the privacy and security benefits of the DDL, for example, by using unqualified language or not mentioning possible security risks.
- Make clear that customers are not required to hand over their devices to law enforcement or other validators.
- Provide accurate advice about whether a plastic licence must be carried and the circumstances in which a plastic card might still need to be shown.
- Ensure messages are consistent and comprehensive across all channels and between Service Victoria, the DTP and the JVO where relevant.
- Ensure that FAQs are easily accessible and cover likely privacy questions including potential security risks and the role and the process for checkers.

**Who:** Both Service Victoria and DTP

**Timeframe:** For pilot and ongoing

The C&E Plan includes communications evaluation measures. For customers, the measure identified is an 'overall customer satisfaction score of >95%'. IIS understands the approach to measuring customer satisfaction is still being developed. We encourage the DTP to include privacy 'satisfaction' in the approach. This could include questions about whether customers has sufficient information to make an informed choice about using a DDL, and if they were confident that privacy and security would be protected.

### Recommendation 4 – Include privacy in pilot evaluation.

Include privacy 'satisfaction' in the evaluation of pilot communications. Issues to consider could include understanding of the QR code content, whether customers had sufficient information to make an informed choice about using a DDL, and if they were confident that privacy and security would be protected.

**Who:** DTP

**Timeframe:** For pilot

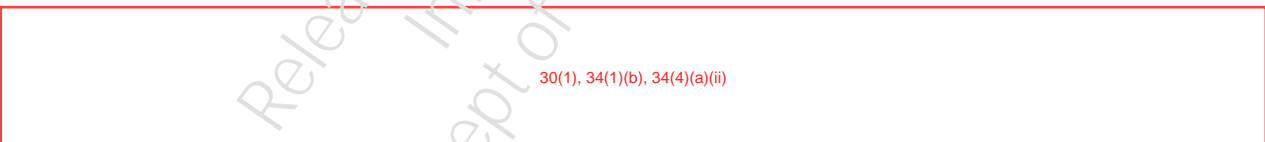
### 5.1.2 Security – IPP 4

IPP 4 requires agencies to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. The DTP and Service Victoria will also be subject to the VPDSF and VPDSS. The VPDSS prescribes a minimum set of mandatory requirements across all security areas including governance, information, personnel, ICT and physical security. The VPDSF provides direction to Victorian public sector agencies or bodies on their data security obligations.

IIS notes that the DTP treats disclosure of R&L data to Service Victoria as though it were a disclosure to a third party; its security due diligence measures take account of this context.



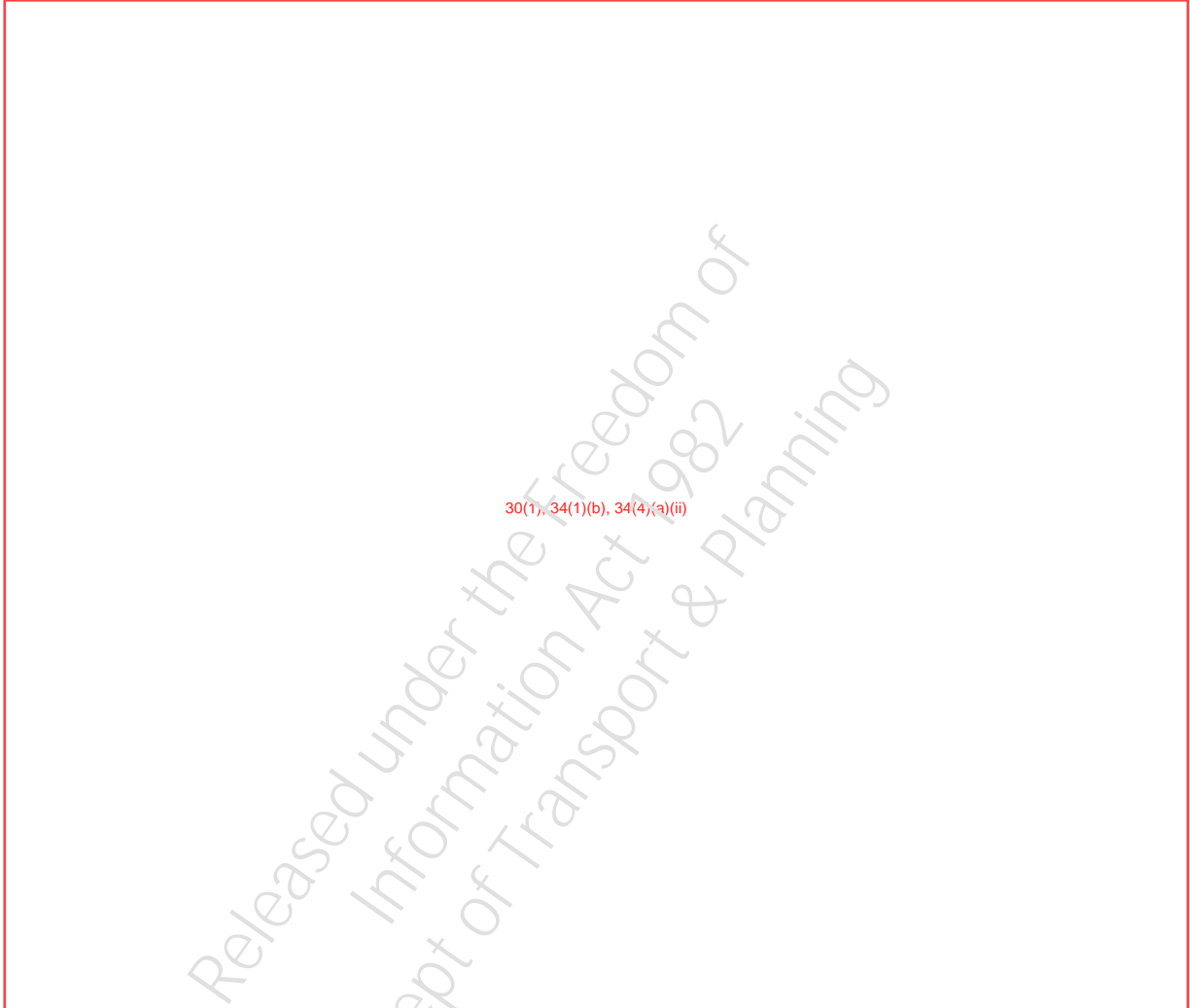
#### 5.1.2.1 System security



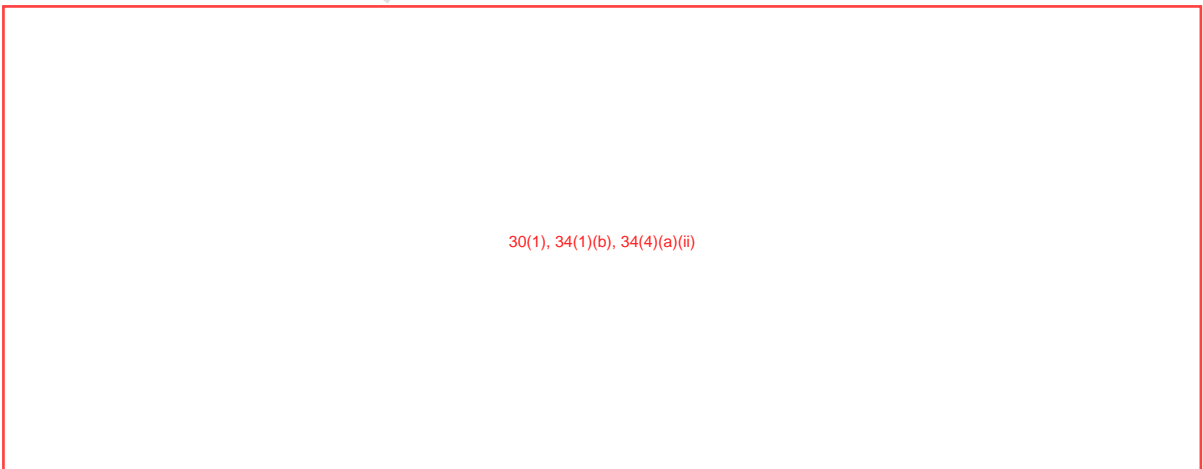
Both Service Victoria and the DTP have noted a number of design features for the project that aim to mitigate the risks. Both also outlined their security approaches and noted specific steps they have taken to identify and manage security risks for the project. IIS notes that the completion of the IVA and agreement on the data classification was crucial in preparation for the regional pilot. We understand that as Service Victoria, the DTP and the JVO gather feedback from the regional pilot, they will also continue to monitor and assess the systems and processes to ensure that it remains efficient and secure.

Security actions that are relevant for this PIA include:

- **Incorporation of Security by Design in the development of the DDL**



- **Security assessments**



30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

**Recommendation 5 – Continue to monitor, assess and update privacy risks in risk register.**

Include privacy risks to individuals using a DDL in the risk register and ensure that these risks are continuously monitored.

**Who:** Both Service Victoria and DTP

**Timeframe:** For pilot and ongoing

**5.1.2.2 Security for users of the DDL**

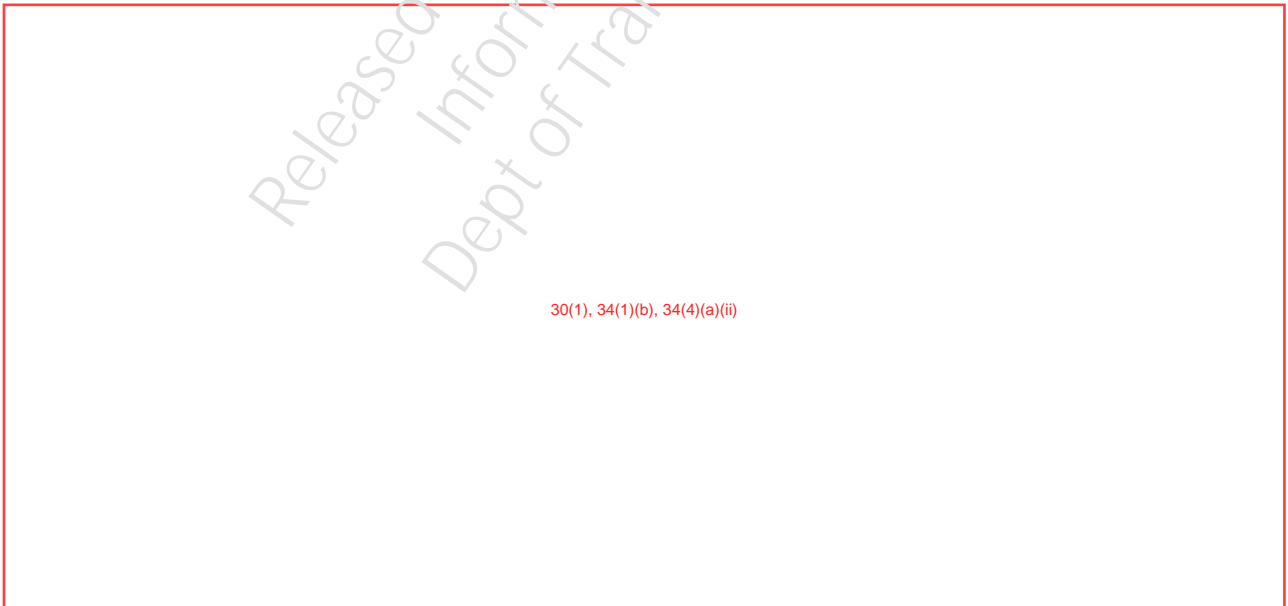
30(1), 34(1)(b), 34(4)(a)(ii)

Features it noted included that:



30(1), 34(1)(b), 34(4)(a)(i)

- A user's unique card number on the DDL is hidden by default.



30(1), 34(1)(b), 34(4)(a)(ii)

### Recommendation 6 – Explore options for limiting address display on the DDL driver licence view.

Explore options for allowing differential display of address on the driver licence view.

**Who:** Both Service Victoria and JVO

**Timeframe:** For full rollout

As noted in [Section 5.1.1.2](#) transparency about security measures and risks is critical to ensuring individuals can make an informed choice about, and have confidence in, using DDLs.

30(1), 34(1)(b), 34(4)(a)(ii)

IIS supports that there should be no requirement for individuals' devices to be handed over to checkers. We note that other jurisdictions that have implemented the DDL (such as NSW) provide that individuals do not need to hand their phone to anyone, including police officers.<sup>8</sup>

IIS recommends that the position be documented as an official policy decision and that appropriate information is included in communications for the regional pilot and full rollout for individuals using DDLs and for checkers including VicPol. IIS notes that the DTP is not currently considering any legislative change to embed the rule, but it may come about in the future only if warranted.

### Recommendation 7 – Document and communicate requirements for the handling of individuals devices for DDL checking.

Document policy decisions that individuals must not be required to hand over their device to DDL checkers including law enforcement. Include clear information on this issue in communications for the pilot and full rollout for individuals using DDLs and for checkers including VicPol.

**Who:** DTP

**Timeframe:** For full rollout

<sup>8</sup> See <https://www.service.nsw.gov.au/privacy-and-digital-licences-and-credentials#licence-or-credential-checkers-handling-your-phone>

### 5.1.3 Access and correction – IPP 6, and privacy complaint handling

Both Service Victoria and the DTP agree that processes for correction as well as complaint handling will have to be worked out to ensure the customers are able to have their issues attended to by the appropriate entity. IIS has been informed that there will be a shared responsibility to rectify issues around the DDL. The DTP will be responsible for providing the licence information and related information about its validity, while Service Victoria will also need to field queries as the DDL will be on the Service Victoria wallet.

The MoU includes complaint handling principles to which the DTP and Service Victoria must adhere. It specifies that both parties will assist each other and cooperate to resolve any complaints or issues and that complaints will be referred to the responsible party.<sup>9</sup> IIS understands that Service Victoria has extensive experience in managing customer services issues and complaints on behalf of its agency partners, including the DTP.

While IIS acknowledges this is not a new issue for Service Victoria, we encourage the DTP and Service Victoria to ensure there is a streamlined 'no wrong door' approach to receiving, and assisting individuals with, privacy queries and complaints related to DDL. At the time of writing the PIA, the materials for privacy complaint handling were still being developed, to be ready for July 2023.

Overall, IIS considers that Service Victoria and the DTP have strong measures in place to deal with privacy enquiries and complaints. Documenting and ensuring staff awareness around these procedures should be a priority before go-live. We also encourage Service Victoria and DTP to continue monitoring the procedures to ensure that they stay fit for purpose.

## 5.2 Governance

### 5.2.1 Project governance

While some development work remains, the DDL Project is now moving to its implementation phases, commencing with the external pilot in July. IIS has been impressed with the emphasis to date on both privacy and security by design in the design and built phases of the DDL. Strong privacy and security protective measures have been included.

However, processes to maintain focus on Privacy and Security by Design did not seem clear. The project governance arrangements have also changed somewhat to reflect that the project is now subject to Cabinet decisions and oversight, and to reflect DTP's engagement of the JVO.

IIS understands that the overarching MoU has now been signed. Detailed agreements, including the DDL transaction journey, that set out the arrangements between the DTP and Service Victoria which includes privacy requirements have also been agreed on. However, the nature of the requirements and processes for ensuring a coordinated best practice approach and for privacy to remain a priority in implementation, evaluation and monitoring phases are not yet clear.

---

<sup>9</sup> Section 8.3 of MoU – Complaint Handling Principles.



### Recommendation 8 – Ensure project governance arrangements include clear privacy roles and responsibilities, including for monitoring privacy outcomes.

Ensure and document a privacy approach that makes clear who is responsible for privacy sign-off for the project, and that monitoring privacy outcomes is included in its project implementation and evaluation plans.

Ensure detailed agreements and ongoing project governance processes include clear privacy requirements and responsibilities for the project, and a comprehensive and coordinated approach to ensuring privacy objectives are met.

**Who:** Service Victoria and DTP

**Timeframe:** For pilot and ongoing

#### 5.2.2 Privacy by Design and future developments

As noted Privacy by Design (PbD) has been a feature of the DDL project development to date. It has been driven by Service Victoria's customer first focus, recent data breaches and the ISO standard. IIS encourages both Service Victoria and the DTP to continue this approach. It will remain relevant as the DDL is implemented and further enhancements are introduced. Particular areas for future privacy focus includes:

- If a notifications feature is introduced, allowing, to the extent possible, for individual choice about whether or not to receive notifications.
- The possible display of licence status and demerit points. Both require further in-depth analysis around policy implications of formal notices/notifications in a digital environment. Where possible, individual choice should also be a key consideration.
- Interoperability with other DDLs, including scanning QR codes without needing the myVicRoads app.
- DDLs available for learners and probationary permits.
- Potential for further privacy features, for example, a record on individuals' devices of which checkers have viewed their licence.

**Recommendation 9 – Continue to adopt PbD in the DDL’s further development.**

Continue the current PbD approach for the DDL, including by conducting further PIAs before making changes to the DDL, for example notifications, or display of status or demerit points, which could impact on individuals’ privacy.

**Who:** Both Service Victoria and DTP

**Timeframe:** Ongoing

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

## 6. Appendix A – Methodology

### 6.1 PIA approach

IIS took the following steps to carry out the PIA:

- *Planning* with the DTP and Service Victoria to confirm the approach, scope and deliverables of the PIA
- *Gathering information* by reading documents and meeting with personnel from the DTP and Service Victoria
- *Analysing the information* against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy good practice
- *Identifying privacy risks* and developing ways to mitigate those risks
- *Drafting the PIA report* and providing this to the DTP and Service Victoria for comment
- *Finalising the PIA report* following feedback from the DTP and Service Victoria.

### 6.2 Documents reviewed

Documents reviewed
<b>DTP documents</b>
1. 230428 digital driver licence communication and engagement plan – v6 final
2. DDL DRAFT Design Standards 20230601 V.03
3. DDL Policy Standards V1.0
4. DTP Risk Matrix
5. IVA DDL 2023 both products
6. IVA DDL 2023 Final
<b>Service Victoria documents</b>
7. Draft Privacy Collection Notice for Digital Driver Licence – 20220504
8. Digital Driver Licence - Transaction Journey (2022.05.16)
9. Operating Service Commitment – Final
10. 221212 LOA assessment – DDL Pilot (final signed)

Documents reviewed	
11.	DDL DoT API Agreement for Service Victoria 20221209 V1.8 - Final
12.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]
13.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]
14.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]
15.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]
16.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]
17.	Service Victoria DTP DDL OVIC 040423
18.	Service Victoria [Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)] assessment
19.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]
20.	[Redacted: 30(1), 34(1)(b), 34(4)(a)(ii)]

### 6.3 Meetings held

Meetings held	Date
Kick-off meeting: <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• DTP personnel</li> <li>• Service Victoria personnel</li> </ul>	3 May 2023
PIA information gathering meeting – Communications and Stakeholder Engagement <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• JVO personnel</li> </ul>	22 May 2023
PIA information gathering meeting – DDL Walkthrough: <ul style="list-style-type: none"> <li>• IIS personnel</li> <li>• Service Victoria personnel</li> </ul>	31 May 2023

## 7. Appendix B – Assessment against the IPPs

The following table sets out IIS’s high-level assessment of the MVP against the IPPs. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii) This will include some health information in form of licence codes. This would be subject to the HPPs in the HRA. IIS notes that the HPPs cover similar issues to the IPPs.

IIS notes that when Service Victoria is collecting data in the context of the DDL, for example, to validate a licence, it is doing so on behalf of the DTP. However, the DTP treats disclosure of R&L data as though it is a disclosure to a third party.

IIS also notes that where our assessment has not identified specific issues for this PIA, that is not meant to indicate there is no privacy work to be done. IIS anticipates that usual privacy compliance and monitoring would occur.

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 1 – Collection</b></p> <p>An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation’s Privacy Policy.</p>	<p>The DDL involves a re-use of existing information the DTP holds, not a new collection for the DTP.</p> <p>The MoU specifies that Service Victoria will be collecting personal information on behalf of the DTP (in the process of loading DDL into the Service Victoria wallet, and in the process of creating/refreshing QR codes).</p> <p>The introduction of DDL is a new way of providing driver licences – it would be at least good practice to update both the DTP’s and Service Victoria’s privacy policies and to ensure privacy collection notices are available and relevant at point of use, for example within the Service Victoria app. The MoU states that Service Victoria must include or provide a link to a DTP collection notice in its app when people are seeking to add the DDL to their wallet.</p> <p>See discussion at <a href="#">Section 5.1.1</a>.</p>

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 2 – Use and disclosure</b></p> <p>Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual's consent, for a law enforcement purpose, or to protect the safety of an individual or the public.</p>	<p>The DTP's use of R&amp;L data for digital driver licence is consistent with the purpose of collection.</p> <p>The IPA also specifically states that Service Victoria undertakes that information shared by the DTP will only be used and disclosed for the purposes set out in the IPA (To provide an alternative digital customer channel for some vehicle registration and driver licensing activities and services of the Department of Transport including under the RSA). Section 90K of Part 7B of the RSA sets out the authorised use or disclosure. Section 90K(a)(vi) allows disclosure in relation to an intergovernmental agreement.</p> <p>No issues identified.</p>
<p><b>IPP 3 – Data quality</b></p> <p>Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.</p>	<p>The DDL should not diminish and may enhance data accuracy of driver licence information.</p> <p>Changes to driver licence details or status will be subject to pilots and roll-out and will be reflected in the DDL quickly.</p> <p>Service Victoria's design of the DDL is in such a way that it does not collect or hold identified personal information except in the limited context of the generation of the QR code. The one source of truth of driver licence information remains with the DTP.</p> <div data-bbox="778 1444 1388 1523" style="border: 1px solid red; padding: 5px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div> <p>No issues identified.</p>
<p><b>IPP 4 – Data security</b></p> <p>Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.</p>	<p>The DTP and Service Victoria have in place detailed security management processes and have commenced or undertaken detailed security risk assessments for the DDL.</p> <p>At this point, there are some outstanding items – see discussion at <a href="#">Section 5.1.2</a>.</p>

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 5 – Openness</b></p> <p>Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation’s Privacy Policy.</p>	<p>Both Service Victoria and the DTP will be updating their privacy policies to reflect the DDL. From a privacy perspective, it will be important to ensure consistency and that individuals are easily able find relevant information to inform their decisions.</p> <p>See <a href="#">Section 5.1.1</a>.</p>
<p><b>IPP 6 – Access and correction</b></p> <p>Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982 (Vic).</p>	<p>The introduction of the DDL should not affect current processes for access and correction. However, Service Victoria and the DTP should ensure respective responsibilities are clear and that processes are built with a ‘no wrong door’ approach.</p> <p>See <a href="#">Section 5.1.3</a>.</p>
<p><b>IPP 7 – Unique identifiers</b></p> <p>A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.</p>	<p>Driver Licence numbers are unique identifiers in terms of the PDPA.</p> <p>Driver licence numbers will appear on the DDL. However, the DDL project does not involve the assignment of new unique identifiers.</p> <p>No issues identified.</p>
<p><b>IPP 8 – Anonymity</b></p> <p>Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.</p>	<p>Not relevant for the DDL – identification is a required part of acquiring or using a DDL.</p>

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 9 – Transborder data flows</b></p> <p>If an individual’s personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.</p>	<p>As far as IIS understands, the DDL processes are contained within Victoria.</p> <p>No issues identified.</p>
<p><b>IPP 10 – Sensitive information</b></p> <p>The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.</p>	<p>Driver licence processes do not involve the collection of sensitive information as defined, but do involve some biometric and health information (See <a href="#">Section 3.6.2</a>). Such information is part of the R&amp;L data that the DTP has already collected.</p> <p>No issues identified.</p>



Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

INFORMATION INTEGRITY SOLUTIONS PTY LTD

PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438

F: +61 2 9319 5754

E: [contact@iispartners.com](mailto:contact@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

ABN 78 107 611 898

ACN 107 611 898



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

**Report: 24 November 2023**

**Department of Transport and Planning (DTP)**

**OFFICIAL: Sensitive**

# PRIVACY IMPACT ASSESSMENT

## SERVICE VICTORIA DIGITAL DRIVER LICENCE PROJECT



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS

## Contents

Glossary	1
1. Executive summary	1
1.1 IIS's overall view	2
1.2 Recommendations	3
2. Introduction	6
2.1 PIA scope	6
2.2 About this report	7
3. Project description	8
3.1 Background	8
3.2 Project objectives and scope	8
3.2.1 Objectives and expected benefits of the project	8
3.3 Project status	9
3.3.1 Completion of external pilot and pilot feedback	9
3.3.2 State-wide release	10
3.4 About the DDL	10
3.5 Participants in the DDL Project MVP	11
3.5.1 The Department of Transport and Planning	11
3.5.2 Service Victoria	12
3.5.3 Joint Venture Operator	12
3.5.4 Checkers – Victoria Police	12
3.5.5 Checkers – other organisations	13
3.5.6 Victorian citizens using a DDL	13
3.6 Nature of systems and information flows	13
3.6.1 Key system components	13
3.6.2 Kinds of information involved	14
3.6.3 Overview of information flows	15
3.6.4 Product changes since pilot release	20
3.7 Legal framework	20
3.7.1 Victorian laws	20

CONTENTS

3.8	Project governance	22
4.	Approach to risk analysis	23
4.1	Inherent privacy risks	23
4.2	Positive privacy aspects	24
4.3	Residual privacy risk level	26
5.	Findings and recommendations	27
5.1	IPP issues or risks	27
5.1.1	Transparency – IPP 1 and IPP 5	27
5.1.2	Disclosure	33
5.1.3	Security – IPP 4	34
5.1.4	Access and correction – IPP 6, and privacy complaint handling	41
5.2	Governance	42
5.2.1	Project governance	42
5.2.2	Privacy by Design and future developments	42
5.3	Additional considerations – negative use cases	44
5.3.1	30(1), 34(1)(b), 34(4)(a)(ii)	44
5.3.2	Fraudulent use cases	47
6.	Appendix A – Methodology	49
6.1	PIA approach	49
6.2	Documents reviewed	49
6.3	Meetings held	51
7.	Appendix B – Assessment against the IPPs	52

## Glossary

Abbreviation or term	Expansion or definition
4(1)(b), 34(1)(b), 34(4)(a)(ii)	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34(1)(b), 34(4)(a)(ii)	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34(1)(b), 34(4)(a)(ii)	30(1), 34(1)(b), 34(4)(a)(ii)
DTP	Department of Transport and Planning
4(1)(b), 34(1)(b), 34(4)(a)(ii)	30(1), 34(1)(b), 34(4)(a)(ii)
4(1)(b), 34(1)(b), 34(4)(a)(ii)	30(1), 34(1)(b), 34(4)(a)(ii)
IIS	IIS Partners and Information Integrity Solutions Pty Ltd
IPA	Information Protection Agreement
4(1)(b), 34(1)(b), 34(4)(a)(ii)	30(1), 34(1)(b), 34(4)(a)(ii)
IPP	Information Privacy Principle
JVO	The DTP's Joint Venture Operator for VicRoads
JWT	JavaScript Web Token
LOA	Level of Assurance
MVP	Minimum Viable Product
MMP	Minimum Marketable Product
OVIC	Office of the Victorian Information Commissioner
PDPA	<i>Privacy and Data Protection Act 2014</i>
PIA	Privacy Impact Assessment
QR Code	Quick Response Code
R&L	Registration & Licensing

0. GLOSSARY

Abbreviation or term	Expansion or definition
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards
VicPol	Victoria Police

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

# 1. Executive summary

The Department of Transport and Planning (DTP), its Joint Venture Operator VicRoads (JVO) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. A DDL will allow a licence holder to access an electronic version of their licence on a mobile device and present it in place of the physical licence. The DDL will be made available through both the myVicRoads and the Service Victoria platforms and apps.

The first phase of the DDL Project was producing a Minimum Viable Product (MVP), which replicated the data and attributes from the existing Victorian driver licence to a digital credential in either the myVicRoads app or the Service Victoria digital wallet. The second phase was testing the Minimum Marketable Product (MMP) via an external regional pilot in Ballarat, which commenced in July 2023. The agencies are now working towards a state-wide release of the DDL, starting in 2024.

The current DDL solution replicates the data and attributes from the existing Victorian driver licence to a digital credential through the Service Victoria digital wallet, with three primary use cases:

- Entitlement to drive
- Proof of identity (i.e., the customer's name and address)
- Proof of being over 18 (i.e., the customer is over 18)

The DDL is one product being delivered in two channels: via Service Victoria and the Joint Venture Operator (JVO). The DTP through the JVO will share its driver licence data with Service Victoria. Due to the quantity and sensitivity of personal information that will be shared with and used by Service Victoria, the privacy impacts of the DDL Project need to be carefully examined.

IIS Partners (IIS) had previously conducted two Privacy Impact Assessments (PIAs) prior to the external pilot – one for Service Victoria's DDL product and one for the JVO's. This PIA report, which focuses on the Service Victoria DDL solution, is an update of the initial PIA (dated June 2023). A separate report will update the June 2023 PIA of the JVO's DDL solution.

The scope of the PIA covers privacy risks associated with:

- Data flows between JVO and Service Victoria
- Security of the information
- Onboarding and user experience in the SV digital wallet
- Features and use cases within the initial release scope
- Any product changes made to the DDL since the pilot
- Core privacy requirements under the Information Privacy Principles (IPPs)
- Potential negative use cases and mechanisms to address them.



## 1. EXECUTIVE SUMMARY

In undertaking this PIA, IIS considered:

- Privacy principles in the *Privacy and Data Protection Act 2014*
- The Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS)
- Relevant legislation such as *Road Safety Act 1986* and the *Service Victoria Act 2018*
- Guidance materials published by the Office of the Victorian Information Commissioner (OVIC) and the Office of the Australian Information Commissioner (OAIC)
- Privacy good practice stemming from IIS's knowledge and experience.

This report:

- Provides background to the project, including key project participants and roles, key systems and information flows, and the relevant legal framework.
- Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.

The PIA methodology is included in the Appendices.

### 1.1 IIS's overall view

Privacy and security have been a key focus for Service Victoria in project design and implementation. IIS has not identified any high-risk privacy issues for the project with respect to implementation of appropriate controls to manage the inherent high risks. Overall, the DDL is likely to benefit individuals and it is being designed in a privacy-friendly way. The issues identified arise in the context of the project stage, which is now turning to implementation and the full-roll out, and the complexity of the project environment.

30(1), 34(1)(b), 34(4)(a)(ii)

- There is significant quantity and sensitivity of personal information involved.
- The project will involve the display of Registration and Licensing (R&L) data in DDLs via individual's devices.
- The data involved includes sensitive biometrics, like driver images as well as R&L details.
- Both the JVO and Service Victoria are offering DDL credentials via their respective apps, consistent with DTP standards. The digital driver licences, while developed independently, are expected to meet the DTP's policy and design standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- Service Victoria's design has taken account of possible security risks for DDL users.

30(1), 34(1)(b), 34(4)(a)(ii)



## 1. EXECUTIVE SUMMARY

- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including how checkers can interact with their devices, or handle personal information displayed via the DDL – can cause concern and jeopardise uptake.

Overall, the DDL has benefited from being designed in a privacy-friendly way. Taking into account the positive privacy aspects such as the emphasis on data minimisation, the avoidance of a new digital footprint, the DDL security features, and expected detailed governance arrangements, we consider that the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, the development of privacy coordination and monitoring arrangements, and close attention to the possible security risks for customers using a DDL.

In our previous June 2023 PIA, IIS identified key privacy risks and issues in the following areas:

- Transparency and privacy complaint handling
- Security
- Privacy governance.

IIS has retained our analysis in relation to the abovementioned areas and added to the analysis any updated information that we have received from Service Victoria and the DTP.

### 1.2 Recommendations

IIS made a total of nine recommendation in our previous PIA. Since then, we note that Service Victoria and the DTP have implemented a number of our recommendations. The status of implementation is displayed in the table below. For this PIA, IIS has a further nine recommendations for Service Victoria and the DTP's consideration as it continues to roll out the DDL state-wide. For ease of reference, the recommendations for this PIA have been listed as Recommendation A, B, C and so forth.

#### Status of previous recommendations

Recommendations	Who	Status
<b>Recommendation 1</b> – Ensure that project agreements and governance arrangements provide for a process for ensuring that privacy messages are consistent and adopt best privacy practice	Service Victoria, JVO & DTP	Implemented
<b>Recommendation 2</b> – Service Victoria privacy policy to include comprehensive DDL information	Service Victoria	Implemented

1. EXECUTIVE SUMMARY

Recommendations	Who	Status
<b>Recommendation 3</b> – Ensure DDL privacy and security information is accurate and does not overstate benefits	Service Victoria, JVO & DTP	Retained – see <b>Recommendation A</b>
<b>Recommendation 4</b> – Include privacy ‘satisfaction’ in the evaluation of pilot communications	Service Victoria & DTP	Implemented
<b>Recommendation 5</b> – Continue to monitor, assess and update privacy risks in risk register	Service Victoria & DTP	Implemented
<b>Recommendation 6</b> – Explore options for limiting address display on the DDL default view	DTP & Service Victoria	Implemented
<b>Recommendation 7</b> – Document and communicate requirements for the handling of individuals devices for DDL checking	DTP	Implemented
<b>Recommendation 8</b> – Ensure project governance arrangements include clear privacy roles and responsibilities, including for monitoring privacy outcomes	Service Victoria & DTP	Implemented
<b>Recommendation 9</b> – Continue to adopt privacy by design in the DDL’s further development	Service Victoria & DTP	Implemented

New / retained recommendations

Recommendations	Who	Timeframe
<b>Recommendation A</b> – Ensure DDL communications, including privacy and security information, are accurate, consistent and fit-for-purpose	Service Victoria & DTP	State-wide release and ongoing

## 1. EXECUTIVE SUMMARY

Recommendations	Who	Timeframe
<b>Recommendation B</b> – Continue to engage with businesses during state-wide release	DTP, Service Victoria & JVO	State-wide release and ongoing
<b>Recommendation C</b> – Continue to monitor customer feedback	DTP, Service Victoria & JVO	State-wide release and ongoing
<b>Recommendation D</b> – Implement pathway to DTP Vulnerable Customers Team as part of enquiries and/or complaint handling process	Service Victoria	State-wide release and ongoing
<b>Recommendation E</b> – Establish formal review mechanism of use of street name verification including process to document identified issues	DTP	Ongoing
<b>Recommendation F</b> – Communicate to <span style="border: 1px solid red; padding: 2px;">34(1)(b), 34(4)</span> <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span> on the importance of keeping their personal details updated	Service Victoria & DTP	Ongoing
<b>Recommendation G</b> – Consult with DTP Vulnerable Customer Team and other relevant <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(i)</span> <span style="border: 1px solid red; padding: 2px;">30(1), 34(1)(b), 34(4)(a)(ii)</span>	Service Victoria & DTP	Ongoing
<b>Recommendation H</b> – Review current materials for licence checkers to identify if more guidance is needed to mitigate against potential fraud cases	Service Victoria & DTP	Within 3-6 months of initial state-wide rollout

## 2. Introduction

The Department of Transport and Planning (DTP), its Joint Venture Operator for VicRoads (JVO) and Service Victoria are working to bring digital driver licences (DDLs) to Victorian residents. The DDL will be made available both through Service Victoria and myVicRoads platforms and apps.

Both the products will leverage data from VicRoads Driver Licence registry, currently operated by the JVO on behalf of DTP. Both products have integration with DTP's driver licence registry using the new technical integration framework that the JVO is implementing as part of the DDL program. DTP provides policy oversight and guidance to ensure that the DDL products are aligned in key areas to deliver a consistent user experience to Victorian motorists.

IIS has previously conducted two PIAs for the Service Victoria DDL solution -- the first for the MVP for the internal pilot (June 2022) and the second for the MMP for the external pilot in Ballarat. This PIA report is an update from the previous MMP PIA (dated June 2023), taking into account Service Victoria's roles in delivering the DDL project for the controlled state-wide release in December 2023. A separate report will update the June 2023 PIA of the JVO's DDL solution.

### 2.1 PIA scope

Service Victoria is responsible for the design of the DDL, in accordance with the DTP's specified standards. DTP is also the data owner of R&L data and will provide the data 30(1), 34(1)(b), 34(4)(a)(ii) 30(1), 34(1)(b), 34(4)(a)(ii) to populate the DDL. The PIA will entail end-to-end consideration of privacy issues that could have an operational impact from the perspective of the DTP, JVO and Service Victoria.

The first phase of the Service Victoria DDL Project involved the production of an MVP through the Service Victoria platform and testing via an internal pilot. The second phase was testing the MMP via an external regional pilot in Ballarat, which commenced in July 2023. There have been certain changes to the DDL since the external pilot.

This version of the PIA is an update to the previous PIA which covers JVO's delivery of the APIs that will deliver data (1), 34(1)(b), 34(4)(a) to the Service Victoria app as well as assessment of any changes or developments made to the DDL post external pilot release that may affect privacy compliance and introduce new privacy risks. The scope of this PIA includes the following additional developments:

- DDL product changes
  - Inclusion of 34(1)(b), 34(4) (allowing both the Service Victoria and JVO credentials to appear simultaneously in both apps, regardless of device)
  - 30(1), 34(1)(b), 34(4)(a)(ii)
- Updates to privacy policies, websites and communications.

The PIA will also discuss potential negative uses of the DDL as well as consider any risks/issues in anticipation of the planned state-wide rollout in December 2023.

In providing this report, IIS makes the following qualifications:

- The PIA considers possible security issues for the project, but we did not undertake detailed investigations or reviews of technical or security features.
- The PIA is based on information gathered from, and provided by, the DTP, Service Victoria and the JVO.
- IIS does not provide legal advice; rather we provide strategic privacy and cyber security advice.

## 2.2 About this report

The report is structured to provide an overview of the DDL project, explain IIS's approach to risk analysis, analyse privacy issues according to the project scope, and provide additional context to the PIA work:

- **Project description** ([Section 3](#))  
Provides background to the DDL Project, key project participants and roles, key systems and information flows, and the relevant legal framework.
- **Approach to risk analysis** ([Section 4](#))  
Sets out IIS's approach to the risk analysis and factors determining the privacy risk level.
- **Findings and recommendations** ([Section 5](#))  
Discusses relevant privacy risks and issues IIS has identified, along with recommendations to mitigate risk and improve practice.
- **Appendix A – Methodology** ([Section 6](#))  
Summarises our methodology, including list of documents reviewed and meetings held.
- **Appendix B – High-level assessment against the IPPs** ([Section 7](#))  
Provides a high-level assessment of the DDL project against the IPPs and notes risks areas, which are discussed in detail in [Section 5](#).

## 3. Project description

### 3.1 Background

Service Victoria and the DTP are working to bring DDLs to Victorian residents. Digital licences offer customers a convenient and secure means to present a driver licence or have their proof of age or identity details verified, where they are required to do so. Three out of six Australian state and territory jurisdictions have either trialled or have a legislation-based DDL. Service Victoria has identified that there are 4.6 million active Victorian customers who use the Service Victoria mobile application, and over 4 million Victorians possess a driver licence. Service Victoria has been progressing delivery of the DDL in collaboration with the DTP.

The DDL replicates data and attributes from an existing plastic Victorian driver licence to a digital credential. Initially there will be three primary use cases:

- Entitlement to drive whilst on the road.
- Casual proof of that user is over 18 and photo for licenced venues and businesses such as supermarkets, convenient stores, tobacco retailers, etc.
- Proof of identity (comprising a customer's name and address).

It will be up to the businesses and organisations who are relying parties to decide whether or not to accept the DDL for these use cases.<sup>1</sup>

The DDL products support verifications where the information is presented on various DDL views using QR code scanning (using the myVicRoads or Service Victoria apps). This feature enables individual and business customers to verify the details presented by a DDL holder without requiring specialised hardware or facial recognition.

A first release of the DDL came in the form of an external pilot which commenced in July 2023. The DTP, JVO and Service Victoria are now working towards a state-wide release, planned for 2024. At this stage, the DDL will be supplementary to the physical driver licence and will not replace it. While most full licence drivers do not need to carry a physical licence, where the existing laws do require this, they remain enforceable. For example, the introduction of DDLs does not change the obligation of motorists such as learner and probationary drivers to always carry their physical licence with them.

### 3.2 Project objectives and scope

#### 3.2.1 Objectives and expected benefits of the project

The DDL is consistent with the Victorian Government's digital strategy, which is expected to deliver cost savings, and better, fairer, and more accessible services, and a digital ready economy.

---

<sup>1</sup> There will be circumstances where a DDL will not be sufficient and a physical driver licence might be needed. For example, the first state-wide release will not allow a business to easily retain a copy of DDL details as part of their existing legal or operational requirements.

The expected benefits of the DDL for Victorian drivers are:<sup>2</sup>

- Freedom – After the pilots, most customers will be able to leave their physical licence and wallet at home.
- Peace of mind – Customers know their DDL is always on their phone as a backup.
- Convenience – 89% of the consulted customers indicated that they believe the DDL to be more convenient than a physical driver licence because they always carry their phone with them.
- Security – Customer’s personal information is protected and only accessible via user login, or 6-digit PIN or biometrics using FaceID/TouchID (if enabled on a customer’s device).
- Privacy – Information sharing can only be initiated by the customer, and the intention is that where circumstances permit, customers will be able to limit the amount of information exchanged.
- Up-to-date data management – Customers using a DDL have access to up-to-date information about the status of their licence; whether it is valid or has expired.

### 3.3 Project status

The DTP, JVO and Service Victoria are taking an iterative approach to the DDL project. Service Victoria and the DTP have undertaken significant development work since the initial MVP in 2022. The design and build of the Service Victoria DDL are complete.

In regard to pilots, one internal pilot was completed and a regional external pilot commenced in July 2023.

The internal pilot was completed to test the DDL end-to-end journey, including identity verification, adding the DDL to the Service Victoria’s Digital Wallet and the communication between Service Victoria and the DTP systems. This is only for full-licence car drivers, and without the QR Code. The DTP did not transfer ‘real’ data to Service Victoria for this pilot.

#### 3.3.1 Completion of external pilot and pilot feedback

The external pilot started in July 2023 in Ballarat. Service Victoria and the JVO promoted the pilot via their websites. Service Victoria asked people to sign up, checked to ensure that there was no duplicate between Service Victoria and JVO, and only sent out invitations specifically to those people. The JVO on the other hand sent out email invitations to its customers in the Ballarat area, requesting their participation. At the time of this PIA, there were approximately 11,000 active Victorian DDLs across both channels.

Both Service Victoria and JVO reported that they received positive feedback on the DDL, with no negative feedback about the product itself.

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

<sup>2</sup> See the 050522.DDL.Pilot.Scope.UC.Roadmap.

### 3.3.2 State-wide release

The project is now moving towards a state-wide release in 2024. IIS has not identified any crucial issues that needs to be addressed prior to the state-wide release. Our recommendations are not time sensitive and should be considered by Service Victoria and the DTP in their future planning of the DDL.

30(1), 34(1)(b), 34(4)(a)(ii)

## 3.4 About the DDL

The DDL will be accessible through the customer's Service Victoria's digital wallet in the Service Victoria app. The app supports selective disclosure, which means the holder has the ability to show and verify subsets of their DDL details – for example, only revealing the fact they're over 18, rather than sharing their exact birthdate, driver licence number, address and other information, as they would be forced to do with a physical licence. These details are verified by a QR code that will be scanned by checkers to verify the licence status.

The DDL will contain features, such as holograms, manual refresh, display of the last refreshed date and time and a watermark.

DDLs will also have additional security features:

- DDLs are protected by the user's phone password or passcode; fingerprint; and/or facial identification (depending on what is used).
- Is only accessible by logging into the Service Victoria app via a user login, biometric identification, or six-digit code.
- The licence validity can be verified via the QR code by non-law enforcement checkers using the Service Victoria app.
- An IRIS barcode is available on the DDL for verification by Victoria Police (VicPol)
- The DDL in the Service Victoria wallet is 'refreshed' to ensure that it is the most up-to-date version. When the licence is refreshed, the information coming from the DTP will overwrite everything that is in the DDL by deleting and replacing it. There are three ways to refresh the licence:

- User initiated – the user manually refreshes the DDL token. A time and date stamp will indicate when the DDL was last refreshed.

- The DDL token itself has a time to live and time to refresh. 30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

If for some reason, the app is unable to do the refresh a notification banner will be presented on the user's device requesting them to connect to the Internet and refresh their licence.



30(1), 34(1)(b), 34(4)(a)(ii)

- Service Victoria also emphasised that the DDL on the phone is effectively a picture only and it is the QR Code that is the critical feature. IIS notes that Service Victoria has undertaken two independent penetration tests on the QR Code and informed IIS that no vulnerabilities have been found with the design and implementation.
- Service Victoria informed IIS if there is any attempt to alter the data or QR Code, the system design means the QR Code will not pass verification. However, Service Victoria noted at this stage, the QR Code can only refresh if the user is connected to the Internet (the image of the licence will still appear on the device when offline).

IIS considers both the Service Victoria and JVO products have been designed and implemented with emphasis on data security and privacy (privacy and security by design). The DTP will also ensure the DDL experience, design, functionality, and features will be same across both DDL channels.

A customer may choose to have both the Service Victoria and myVicRoads apps on their device, from which they can access the DDL.

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

At this point, the products are not interoperable (this will be taken up in future phases). This means that the JVO QR code can only be scanned with the JVO app and vice versa with the Service Victoria app. Additionally, the apps include a 'deep' link that will direct the verifier to the correct app.

## 3.5 Participants in the DDL Project MVP

This section sets out the participants in the DDL project.

### 3.5.1 The Department of Transport and Planning

The DTP operates and coordinates Victoria's transport network, the delivery and upgrade of transport infrastructure, as well as the reforms to road safety policy, regulatory and legislative environment. The DTP will remain the owner of the R&L data.

The DTP is also the policy owner of driver licensing policy. All the elements that relate to licence information, entitlement to drive, safety and roads will remain with the DTP. The user's licence features and potential changes (e.g., addition of a licence, expiration, suspension) are managed on the DTP's side, and JVO and Service Victoria only reflects those changes through the DDL.

The DTP provides policy oversight and guidance to ensure that the DDL products are aligned in key areas to deliver a consistent user experience to Victorian motorists.

### 3.5.2 Service Victoria

Service Victoria was created by the Victorian Government to modernise Victorian customer's online government services and make it easier for people to complete more online services more often from the comfort and safety of their own homes. Customers can access more than 100 government services through Service Victoria.

Service Victoria is responsible for the solution delivery through the Service Victoria app (as one of two channels), as the JVO will also deliver its own version through its myVicRoads app. Service Victoria is responsible for the maintenance of the app and ensuring that the right security, privacy and compliance features are in place. Service Victoria is also responsible for the communications with customers and will provide a digital channel for customer feedback about the DDL via a feedback mechanism on the app to regarding the addition of the DDL to the Service Victoria wallet. Customers can provide both quantitative and qualitative feedback.

Over time, the Service Victoria digital wallet is expected to include a wide range of Victorian government licences and permits.

### 3.5.3 Joint Venture Operator

The JVO is responsible for customer service in relation to R&L and operational activities (except in relation to complex customers), initial level of customer complaint, and management of the DTP's IT systems. [Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)

Additionally, the JVO is providing and operationally supporting the APIs required to integrate with Service Victoria.

The JVO is also responsible for producing a DDL in its app.

### 3.5.4 Checkers – Victoria Police

VicPol is a key stakeholder for the DDL and is working with DTP to identify and resolve any issues.

The external regional pilot was used to test the efficacy of, and seek feedback on, the VicPol app already available to check the barcode, which IIS understands contains only the licence number. VicPol only checks the DDL as an initial check. It will continue to verify the physical driver licence [Redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

[Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)

IIS understands that no issues were raised VicPol during the pilot and that they were generally pleased with the ease of using the solution. The DTP will continue to engage with VicPol to identify any needed modifications of police processes if/when the DDL becomes a replacement for a hard copy driver licence.

### 3.5.5 Checkers – other organisations

There will be a number of businesses that need to verify licences or identification. These include:

- National Retailers Licensed venues such as bars, pubs, nightclubs, and restaurants
- Hotels
- Petrol service stations
- Supermarkets and grocery stores
- Convenience stores
- Tobacco retailers
- Pharmacies
- Banks
- Australia Post
- Licensed premises, parcel pickup and delivery businesses, retailers offering click and collect, credit options and equipment hire.

IIS notes the initial focus will be on small businesses that do not need to retain documentary evidence of identity. Such requirements might be considered in further iterations of the DDL.

### 3.5.6 Victorian citizens using a DDL

At the time of writing, there were approximately 11,000 active Victorian DDLs across both the Service Victoria and JVO channels. The current DDL solution is only available for drivers with a full licence including car, motorcycle, light, heavy vehicles. The state-wide release is planned for 2024.

The DTP expects the DDL will be extended to all licence holders including probationary drivers and learner drivers in further stages of the project.

## 3.6 Nature of systems and information flows

### 3.6.1 Key system components

#### 3.6.1.1 The DTP

The main DTP systems involved for the DDL are:

- 
- 

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

### 3.6.1.2 JVO

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

, 34(1)(b), 34(4) The APIs will allow 30(1), 34(1)(b), 34(4)(a)(ii) driver licence data to be retrieved by the front-end mobile apps developed by the JVO and Service Victoria.

### 3.6.1.3 Service Victoria

To build the DDL, Service Victoria is leveraging existing infrastructure previously used within Service Victoria, for example its digital wallet. An advantage here is that Service Victoria has confidence in the systems, including because a number of components have already gone through security audits.

The Service Victoria platform hosts the app. The customer must download the app on their device and create a Service Victoria account to be able to generate a DDL and hold it within their digital wallet.

### 3.6.1.4 Licence holders

Licence holders will use their own devices to set up, or use, a Service Victoria account, and to add a DDL to the Service Victoria digital wallet within the mobile app.

## 3.6.2 Kinds of information involved

### 3.6.2.1 Personal information

The kinds of personal information to be shared by the DTP is the same as what currently appears on the plastic licence. This is:

- Full name
- Date of birth
- Full address
- Signature
- Photo

- Licence number
- Licence expiry date
- Licence type (car/bike/dual)
- Licence proficiency (full/probationary)
- Licence category (heavy vehicle categories)
- Licence conditions
- Card Number
- Issue Date
- Licence Status.

The DDL QR Code (when scanned) will also display information which will vary depending on the particular verification scenario. The aim is that more sensitive licence information will only be available under the photo of the licence when a user opts to display their full licence.

### 3.6.2.2 Sensitive information and health information

The DTP will also share conditions included on driver licences (e.g., alcohol interlock device, driver aids or vehicle modifications, etc.). One of the conditions is a letter 'S' that indicates glasses or corrective lenses. IIS considers that in this limited circumstance, the condition could meet the definition of health information in the *Health Records Act 2001*, although practically speaking the privacy risk is low.

The DTP will also share biometric information with Service Victoria in the form of the licence photo and signature. Biometric information is not explicitly contained in the definition of sensitive information in the *Privacy and Data Protection Act 2014*. However, it is considered sensitive information under the *Privacy Act 1988* (Cth) and OVIC advises organisations to consider treating biometric information as 'delicate information' and to handle it cautiously.<sup>3-4</sup>

### 3.6.3 Overview of information flows

At a high level, the arrangements for the DDL are expected to involve the following:

- 30(1), 34(1)(b), 34(4)(a)(ii)

<sup>3</sup> Please refer to the definition given by OVIC: "*Delicate information*' refers to personal information that is of a private or personal nature, or information that the individual it is about would likely regard as requiring a higher degree of protection.", available at [https://ovic.vic.gov.au/book/key-concepts/#Sensitive\\_and\\_delicate\\_information](https://ovic.vic.gov.au/book/key-concepts/#Sensitive_and_delicate_information).

<sup>4</sup> See <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>.

- As noted, Service Victoria will be using its existing infrastructure and processes for Service Victoria accounts and digital wallet to support the DDL. It will add a QR code generation process. Customers will use an existing Service Victoria account, or set one up, requiring consent-based identity verification (at a level of assurance two in accordance with its Identity Verification Standards).<sup>5</sup> Service Victoria is designing its system to allow for secure ‘blind’ pass through of data between the DTP to a customer’s device. It will ‘see’ personal information only at the QR code generation step and will not retain any personal information, including in audit logs.
- As an additional validation measure, customers will have to input their street name as part of the process in verifying their driver licence details (in order to access the DDL).
- Customers can choose to show their DDLs to checkers (law enforcement agencies, or businesses seeking proof of identity or age).

The following section describes in more detail the information flows relating to the creation of a Service Victoria account and the creation of a DDL in the Service Victoria app. It also describes the information flows when a QR Code is generated and verified using the Service Victoria app (both by the customer and the checker).

Steps for the user	Back-end processes
Log into the app / create an account	
<p>The customer logs into the app.</p> <p>If the customer doesn't have an account, they create one and start by entering the email address, password, first and second name in required fields. The customer creates a six-digit PIN and can set up biometric authentication (such as their face or fingerprint) – this is not stored on the app.</p>	<p>If an account is created, email address and mobile phone (if provided) are verified via the use of a one-time passcode.</p>
Add the DDL to the wallet	
<p>In the ‘My Wallet’ tab of the app, there will be an ‘Add Driver Licence’ button. The customer taps on this.</p> <p>At this point the customer provides their consent to verify their ID documents and Australian driver licence.</p>	<p>This will trigger the normal flow in the back end for when there has been a request to add something to the wallet.</p> <div data-bbox="767 1704 1374 1832" style="border: 1px solid red; padding: 5px; text-align: center; color: red;">                     30(1), 34(1)(b), 34(4)(a)(ii)                 </div>

<sup>5</sup> See <https://service.vic.gov.au/about-us/service-victoria-identity-verification-standards>.

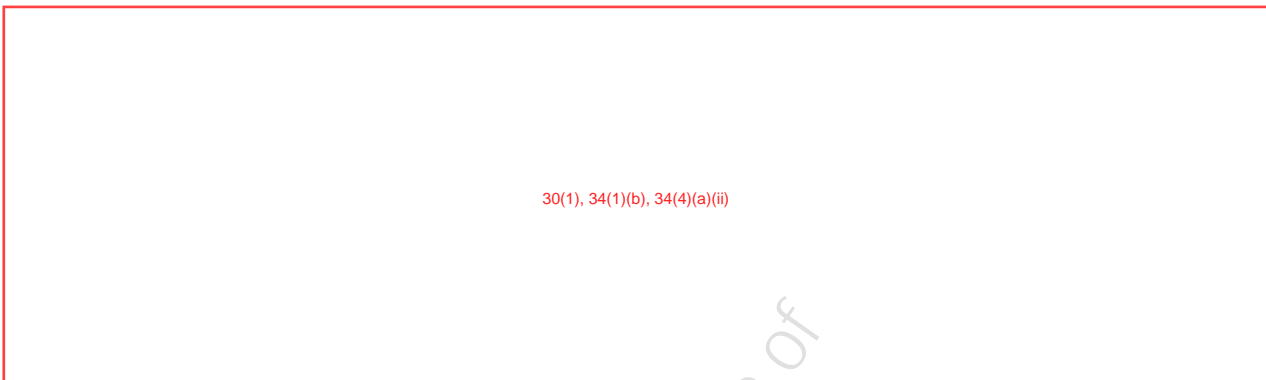
Steps for the user	Back-end processes
Verify identity with choice of ID – If customer does not have a saved Electronic Identity Credential (EIC)	
<p>The customer provides consent to verify their identity at a level of assurance two (LOA2). This requires the customer to provide two satisfactory identity documents from the list below:</p> <ul style="list-style-type: none"> <li>● a full Australian birth certificate; or</li> <li>● a full Australian passport; or</li> <li>● a foreign passport with a valid Australian visa; or</li> <li>● an ImmiCard; or</li> <li>● an Australian Citizenship Certificate; or</li> <li>● an Australian driver licence; or</li> <li>● a Medicare card.</li> </ul>	<p>The customer undergoes identity verification. (1)(b), 34</p> <div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
<p>The user is presented with the choice to create an ongoing EIC that will be valid for 10 years.</p>	<p>If the customer consents to creating an ongoing Electronic Identity Credential, 30(1), 34(1)(b), 34(4)(a)(ii)</p> <div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>
Validate EIC – If customer has an account with an existing EIC	
<p>If the customer has an account with an existing EIC at Level of Assurance (LOA2) or above, Service Victoria validates the identity.</p>	<div style="border: 1px solid red; padding: 10px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>

Steps for the user	Back-end processes
Verification of driver licence details (in order to access DDL)	
<p>The customer is presented with a screen requiring them to enter the following information:</p> <ul style="list-style-type: none"> <li>• Name (as it appears on their physical driver licence)</li> <li>• Street name</li> <li>• Licence number</li> <li>• Licence expiry</li> <li>• Unique card number (optional)</li> </ul>	<div style="border: 1px solid red; height: 400px; width: 100%;"></div> <p style="text-align: center; color: red; font-size: small;">30(1), 34(1)(b), 34(4)(a)(ii)</p>
Loading DDL	
	<p>Upon verification, the personal information (including the image of the individual) is encrypted</p> <div style="border: 1px solid red; text-align: center; padding: 5px; margin: 10px 0;"> <p style="color: red; font-size: small;">30(1), 34(1)(b), 34(4)(a)(ii)</p> </div> <p>As soon as the DDL is added to the wallet, the name data is deleted from Service Victoria's platform.</p>
<p>The customer can now access the DDL from the Service Victoria wallet.</p>	<div style="border: 1px solid red; text-align: center; padding: 5px; margin: 10px 0;"> <p style="color: red; font-size: small;">30(1), 34(1)(b), 34(4)(a)(ii)</p> </div>



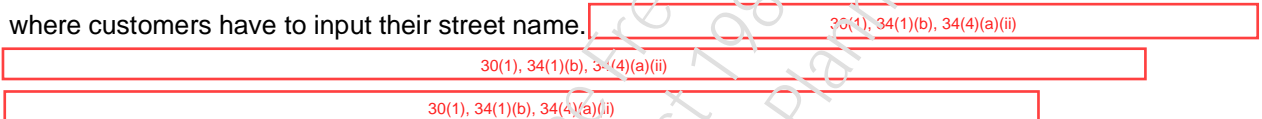
Steps for the user	Back-end processes
QR Code generation and verification	
<p><b>Generating a QR Code:</b></p> <p>The user will be given the choice to decide on different sharing options. This will allow them to determine how much of their driver licence information they'd like to show to non-law enforcement checkers.</p>	<p>30(1), 34(1)(b), 34(4)(a)(ii)</p> <p>The QR code that is generated is only valid for two minutes before it refreshes and the encrypted data on the platform is deleted at the same time.</p>
<p><b>Verifying a QR Code:</b></p> <p>Businesses that require proof of age will be able to scan the QR code to verify its validity and to see the licence information (what is shown will depend on the policy about differential display, and then on what the DDL user chooses to display).</p>	<p>30(1), 34(1)(b), 34(4)(a)(ii)</p>

### 3.6.4 Product changes since pilot release

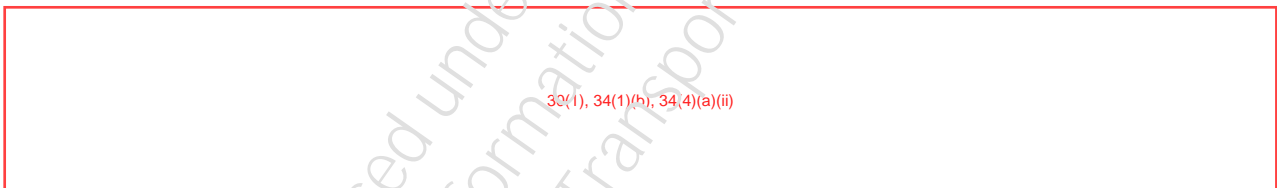


#### 3.6.4.2 Street name verification

As mentioned above, an additional field has been added to the verification of driver licence details stage – where customers have to input their street name.



#### 3.6.4.3 Device limitations



## 3.7 Legal framework

### 3.7.1 Victorian laws

The DDL project must comply with the following relevant laws.

#### 3.7.1.1 Privacy and Data Protection Act 2014

The *Privacy and Data Protection Act 2014* (PDPA) regulates the handling and protection of personal information by Victorian public sector organisations. Organisations subject to the PDPA must comply with the Information Privacy Principles (IPPs) that contain requirements across the information lifecycle. Part 4 of the PDPA gives the Victorian Information Commissioner the power to prescribe security requirements pertaining to public sector information and information systems through the Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS).

### 3.7.1.2 Health Records Act 2001

The *Health Records Act 2001* (HRA) and its Health Privacy Principles (HPPs) regulate the collection, handling and protection of health information, which includes information or opinion about the physical or mental health or disability of an individual.<sup>6</sup>

### 3.7.1.3 Road Safety Act 1986

The *Road Safety Act 1986* (RSA) is the main piece of legislation that regulates the use of roads, registration of vehicles and driver licensing in Victoria.

Part 7B of the RSA contains the protective framework for relevant information, including the allowed purposes for use and disclosure of relevant information, the exceptional circumstances for the use and disclosure of relevant information, the uses of relevant information for verification purposes, etc. Part 7B applies to Service Victoria because it has requested access to the driver licence information held by the DTP where the information may identify an individual or allow an individual's identity to be ascertained.

The DTP and Service Victoria have had a Service Agreement since 2017. For the DTP to disclose the data to Service Victoria, the DTP and Service Victoria also had to enter into an Information Protection Agreement (IPA) in accordance with section 30N of the RSA. No legislative changes to the RSA are needed for the DDL, as the recent amendments of the RSA and the *Service Victoria Act 2018* are sufficient to deliver the solution. In the longer term, changes to RSA may be necessary to incorporate digital services.

### 3.7.1.4 Service Victoria Act 2018

The *Service Victoria Act 2018* provides for the delivery of government services to the public by Service Victoria and provides a regulatory framework for the provision of identity verification functions by the Service Victoria CEO. Importantly, the Act establishes that the Service Victoria CEO must comply with identity verification standards when verifying identity. These standards are set out separately to the legislation and provide a consistent and secure identity verification framework for people transacting with the Victorian Government through Service Victoria. Among other things, the *Service Victoria Amendment Act 2022* added new provisions supporting digital delivery of Victorian licences.

### 3.7.1.5 Charter of Human Rights and Responsibilities Act 2006

The *Charter of Human Rights and Responsibilities Act 2006* (the Charter) is a Victorian law that sets out the protected rights of all people in Victoria as well as the corresponding obligations on the Victorian Government. The DTP will be conducting a Charter assessment with particular focus on engagement or limitation of the right to privacy.

---

<sup>6</sup> The HPPs are substantially similar to the IPPs. For the purposes of our privacy analysis in Section 5, IIS has focused on the IPPs.

### 3.7.1.6 Road Safety (Drivers) Regulations 2019

Regulation 63 of the Road Safety (Drivers) Regulations 2019 describes the details that driver licence or learner permit documents must contain, including the identification number, the person's first name, second and third initials (if any) and family name; a photograph of the person; the person's residential address; the person's date of birth; a reproduction of the person's signature; the category or categories of driver licence; its expiry date; and the code of any condition to which the licence or permit is subject.

## 3.8 Project governance

In November 2021, the Interdepartmental Committee (IDC) endorsed preliminary detailed scoping work to support an MVP release strategy. At project initiation, Service Victoria provided the DTP with an initial delivery agreement. This agreement specified the scope and timeline for work. IIS understands that the authorising structure for the project has now changed. Policy governance matters sits with the DTP and Service Victoria is one of the delivery channels.

As the project has continued to progress, several governance arrangements that have been put in place includes:

- Ministerial oversight via monthly ministerial meetings
- Steering committee with senior staff from Service Victoria and the DTP
- Working groups sitting under the steering committee with weekly meetings
- Development of DDL standards set by the DTP which include the DDL Policy Standards and the DDL design standards.

These arrangements are now moving to a more formal partnership arrangement with the DTP, taking account of the fact that the authorising governance will be coming from Cabinet, as well as the JVO, which will see modernisation of its systems and processes. The arrangements include:

- Ministerial oversight
- A Memorandum of Understanding (MoU) between Service Victoria and the DTP, setting out overall principles on how the relationship works and a high-level governance framework
- Operating service commitment
- Transaction journey documents
- Information Protection Agreement.

These documents and processes set expectations and respective roles and responsibilities, including with respect to privacy.

IIS understands the MoU remains in effect and that the IPA was updated in June 2023. We also understand that the structure of project steering committee and related working groups and consultative processes will continue.

## 4. Approach to risk analysis

In undertaking this PIA, IIS considered:

- The IPPs in the PDPA
- Guidance materials published by the OVIC and the OAIC
- Privacy good practice stemming from IIS's knowledge and experience.

The PIA focuses on privacy risks that are introduced or heightened by the DDL Project, rather than privacy risks for existing processes to issue and use driver licences.

This section assesses the project's residual privacy risk level, by weighing the inherent privacy risks against the existing privacy positive aspects.

The following section discusses the project's privacy issues and risks identified in detail and makes recommendations to mitigate the risks.

### 4.1 Inherent privacy risks

IIS's risk analysis approach begins with identifying the inherent privacy risks. Inherent privacy risks arise from:

- The nature of the personal information to be collected and managed – for example, its quantity, sensitivity, and the potential (including value) for, and consequences of, misuse.
- The range of people from whom the information may be collected.
- The context in which personal information is handled – for example, senior management commitment to privacy, staff privacy skills and experience, the technical systems involved and the nature of the project.
- The extent to which information is accessed or handled by third parties.
- The likely community and/or media interest in the privacy aspects of the project.

30(1), 34(1)(b), 34(4)(a)(ii)

- There is significant quantity and sensitivity of personal information involved.
- The project will increase likelihood of potential exposure of sensitive personal information data to the Internet via apps and APIs.
- The project will involve the display of R&L data in DDLs via individual's devices.
- The data involved includes driver images as well as R&L details.

- The DDL project environment is complex, with both Service Victoria and the JVO offering DDL credentials via their respective apps, under the guidance of the DTP. The apps, while developed independently, are expected to meet the DTP's policy and design standards, and to have a consistent 'look' and 'feel'. However, the apps vary in some key ways, which individuals might find confusing or difficult to assess from a privacy perspective.
- Service Victoria's design has taken account of possible security risks for DDL users. However, there is still potential for risks to be greater than expected or for unforeseen risks to arise and so calls for a need for risks to be monitored on an ongoing basis.
- While Victorians are reasonably familiar with, and interested in using DDLs, insufficient clarity or inadequate information about the possible privacy risks – including the differences in the two channels, how checkers (aka 'verifiers') can interact with their devices, or handle personal information displayed via the DDL – can cause concern and jeopardise uptake of the solution.

## 4.2 Positive privacy aspects

IIS considers that the DDL Project has important positive aspects that support privacy and minimise the inherent risks associated with the project. These are outlined below:

### Positive privacy aspects with the project/solution design

- Service Victoria has followed the key privacy enhancing strategy of data minimisation – it will handle minimal personal information and will not retain any such information. In particular:
  - When the DDL has been added to the Service Victoria wallet, the only thing stored in Service Victoria's platform is a linking key 34(1)(b), 34(1)(c) in the wallet database. This indicates that the user has a driver licence in their wallet, and the platform uses that linking ID to get the driver licence information from the DTP.
  - The path through Service Victoria's platform from the DTP to the app is automated; no licence information is stored, and no Service Victoria personnel will have access to it as it passes through the platform. Service Victoria specified that there are no 'dead letter queues' or any other place where personal information may inadvertently be stored (including in log files).
- The DDL project design appears to avoid the risk of a new digital footprint, in that neither Service Victoria or the DTP will have any detailed records that would enable them to track when, or to whom, a customer presents their DDL for checking. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii)
- The DDL does not rely on the creation of duplicate stores of personal information. 30(1), 34(1)(b), 34(4)(a)(ii)  
30(1), 34(1)(b), 34(4)(a)(ii) This means the DTP data remains the single 'source of truth' for driver licence information.
- The information embedded in the QR code is information that have been validated by Service Victoria and is only available for display without refresh for a limited period of two minutes.

## Governance and risk management

- Service Victoria and DTP have indicated a commitment to privacy and appear to have this in mind as the project design is finalised and as it progresses to implementation, this includes having appropriate governance arrangements in place to support privacy requirements.
- The arrangement between the DTP and Service Victoria is governed by an MoU and IPA (as required under Part 7B of the RSA). These documents contain the roles and responsibilities of both parties and in particular the privacy and security obligations.
- Service Victoria has undertaken considerable consultation and design work in collaboration with the DTP.
- The DTP has liaised with Service Victoria to assess its security culture and risk management in the context of the DDL.
- Service Victoria's design has taken account of possible security risks for DDL users. Service Victoria 30(1), 34(1)(b), 34(4)(a)(ii) to perform a well architected framework review of the solution and has had two independent penetration tests conducted against the build.
- DTP has completed an Information Value Assessment incorporating feedback from Service Victoria's own Information Value Assessment.
- DTP has conducted independent security assessment processes.

## Privacy advantages for DDL users over the existing plastic driver licence

- The DDL is potentially more secure in that it is protected by device and Service Victoria app security measures, including password or PIN protection.
- The DDL includes a range of other security features and further work is being undertaken to identify if other measures are needed.
- If a DDL is reported stolen or lost and has been cancelled by the DTP, this will be reflected in the DDL and the QR code will not be able to be refreshed and verified.
- A customer's DDL can be verified in real-time. This means data can be instantly verified by scanning the QR code displayed on the DDL within the Service Victoria app.
- DDL users will have some choice about what information they display to verifiers – the app will have three 'cards', which will display only relevant details, for example, the identity card will display the customer's photo, date of birth, and address, but not their driver licence details.

### 4.3 Residual privacy risk level

Overall, the DDL is likely to benefit individuals and it is being designed with privacy and trustworthiness as key considerations. Rather, the issues identified arise in the context of the project stage and the complexity of the project environment.

In summary, with a number of important issues to manage both during and after state-wide rollout, IIS considers the residual privacy risk level is medium. Privacy risks are likely to be within manageable levels, subject to clear and detailed privacy communications, continuous privacy coordination and monitoring arrangements, and close attention to and monitoring of the possible security risks for customers using a DDL.

Released under the Freedom of Information Act 1982  
Dept of Transport & Planning

**DRAFT**



## 5. Findings and recommendations

This section discusses relevant privacy risks and issues that IIS has identified during the PIA.

IIS has retained our analysis from the previous June 2023 PIA and added to the analysis any updated information that we have received from Service Victoria and the DTP.

IIS made a total of nine recommendations in our previous PIA. Since then, we note that Service Victoria and the DTP have implemented a number of our recommendations. The status of implementation is displayed in each recommendation box. In key areas where we have included further recommendations, these are titled as Recommendation A, B, C and so forth.

IIS has not identified any areas of non-compliance with privacy or other legislation. The recommendations focus on ensuring privacy best practice. For each recommendation, we have suggested who would be responsible for carrying out the recommendation (the DTP, Service Victoria or both).

### 5.1 IPP issues or risks

A high-level analysis of the DDL project against the IPPs is at [Appendix B](#). IIS considers the DDL project would be mostly consistent with the IPPs. For example:

- The project operates within the existing legal framework.
- Service Victoria will be authorised to collect and handle limited, generally encrypted, personal information consistent with the Service Victoria Act 2018.
- Anonymity is not practicable.
- The project will operate within Victorian borders.

The main IPPs where IIS has identified issues are in relation to transparency and openness, disclosure, security, access and correction, and privacy complaint handling.

#### 5.1.1 Transparency – IPP 1 and IPP 5

Transparency provisions in the IPPs aim to allow individuals to make informed choices about providing information or using a service and to have a general understanding of how information about them is being handled. Transparency is both a matter of compliance as well as key to building public confidence and trust in the DDL. The IPPs provide two transparency mechanisms:

- Specified details, usually a collection notice, provided at the point personal information is collected or as soon as possible thereafter (IPP 1.3).
- General information available about the type of personal information agencies collect and hold and how it is managed (IPP 5.1).

#### 5.1.1.1 Privacy collection notice and privacy policy

In keeping with its policy and oversight roles for the DDL and the 'one licence, two channels' approach, the DTP will ensure consistency in collection notices for the Service Victoria and myVicRoads apps.

In regard to the collection notice, IIS notes that Section 12.1 of the MoU states that collection notices will be provided by the DTP. IIS has been informed that a layered approach to the notices apply:

- Service Victoria's collection notice will refer to the collection of data necessary to add a DDL within the Service Victoria app.
- The DTP's collection notice will refer to the collection and use of R&L information.

IIS reviewed the collection notice currently available on Service Victoria's website which will be updated to reflect state-wide release (noting that it now currently only refers to the pilot). IIS supports the clarity of the notice and did not find any issues under IPP 1.3. The notice uses plain English and gives a reasonably detailed overview of the Service Victoria DDL. The collection notice should be updated as needs arise.

IIS understands Service Victoria will continue to develop its privacy materials in consultation with DTP and following the established Service Victoria style guide and pattern (in accordance with the MoU). IIS notes that the DTP is inclined to follow Service Victoria's approach and will ensure that the JVO aligns with such approach.

IIS notes a working group made up of personnel from DTP, JVO and Service Victoria is in place to ensure that all agencies are on the same page in relation to the DDL state-wide rollout. This includes ensuring any privacy messages or external communications from both Service Victoria and JVO have similar content and use consistent language. IIS understands that this has been agreed by all parties.

We also reviewed Service Victoria's updated privacy policy currently live on its website. The privacy policy now includes a distinct section on the DDL which details the handling of personal information when a customer adds a DDL, the QR code functionality, activity logs as well as what happens when a device is stolen. IIS finds the privacy policy to be clear and comprehensive. As such, we make no further recommendations.

## Status of recommendations from previous PIA

### Recommendation 1 – Ensure that project agreements and governance arrangements provide for a process for ensuring that privacy messages are consistent and adopt best privacy practice

Establish project agreements and governance arrangements to ensure that privacy messages delivered by the DTP, JVO and Service Victoria are consistent, comprehensive and adopt best practices approaches.

**Who:** Both Service Victoria and DTP

**Timeframe:** For full rollout and ongoing

**Status:** Implemented

### Recommendation 2 – Service Victoria privacy policy to include comprehensive DDL information

Include comprehensive DDL information for the full public rollout in Service Victoria's privacy policy.

Include an additional 'extra privacy information' section on the information handling for DDLs, which should cover matters such as:

- Collection and handling of information for identity verification
- Activity logs
- Data security, including steps to take if a device is lost or stolen
- QR Codes, including what they contain and how refreshed
- Licence or credential checker handling a device
- How to report a device as lost or stolen to Service Victoria and/or to VicPol.

**Who:** Service Victoria

**Timeframe:** For full rollout

**Status:** Implemented

#### 5.1.1.2 Public communications and education

In addition to the specific requirements in the IPPs, active public awareness and education for DDL users and verifiers will support transparency about the project, and support individuals' ability to exercise their privacy rights and to use a DDL safely.

IIS is encouraged by the work DTP, JVO and Service Victoria have done to date in this area. In keeping with its role in ensuring the DDL experience, design, functionality and features will be same across both channels, the DTP is taking the lead on DDL communications and engagement.

IIS notes that Service Victoria, the DTP and the JVO have developed a Communications and Engagement Plan (the C&E Plan).<sup>7</sup> The C&E Plan includes the narratives and key messages for the regional pilot as well as communications and engagements tactics and timings in preparation for the full rollout. The narratives and key messages provide a good high-level overview of the solutions offered by both Service Victoria and the JVO.

The Communications Team is also working on a number of collaterals to continue to promote public awareness and educations which include updating the current FAQs, publishing factsheets and an instructional video for users as well as briefing packs. IIS considers these efforts to be important in not only driving uptake but to ensure that Victorians are adequately informed about the DDL and its processes.

IIS notes Service Victoria has implemented some of the items in the C&E Plan, such as updating its webpage on the DDL to include FAQs, and publishing a Guide for Licence Checkers to support business awareness of DDLs and how they could use it in practice, including the steps to verify the licence, identity, or age cards. In addition, as part of the broader rollout of the DDL, IIS understands Service Victoria and the JVO are planning to increase their engagement with businesses (that are licence checkers) in order to guide and support them. IIS supports this initiative and recommends for Service Victoria to continue to its engagement with customers to better understand their pain points and needs but also as an opportunity to educate businesses about the licence verification process.

Additionally, IIS makes some further suggestions which would enhance the clarity and accuracy of privacy messages:

- Specifying the difference in approach between the DDL when enrolling via Service Victoria and JVO (we recognise the DTP may be better placed to coordinate this).
- Provide information that is more tailored for customers about how to use the DDL and how a DDL is verified, as well as explicitly informing users that the licence image on the Service Victoria wallet is simply a replicated image and that the verified licence details are encrypted within the QR Code.
- Adequate information on what sharing options are available for the DDL, how to generate the QR Code, what the process is when allowing checkers to sight a DDL user's QR code and what their rights are.

30(1), 34(1)(b), 34(4)(a)(ii)

---

<sup>7</sup> Communications and Engagement Plan (April 2023).

- Make clear to customers DDLs might not be accepted in all circumstances at least initially, including overseas. For example, verifiers might not take up the QR code scanning option, or they need to take a copy of a licence. While it might be OK to 'leave your plastic in your pocket', it might be clearer to encourage customers to have the plastic card with them during the initial rollout period.<sup>8</sup> In addition, while IIS understands that customers do not need to have a licence with them, except where there is a legal requirement to carry, e.g., learners and probationary drivers, it might be helpful to make this clear.

The above suggestions and those listed in Recommendation A below are based on best practice considerations. Service Victoria and DTP should continue to bear them in mind as they develop and update the relevant communications materials.

The C&E Plan includes communications evaluation measures. For customers, the measure identified is an 'overall customer satisfaction score of >95%'. Service Victoria has so far received positive feedback on the DDL. However, there is no empirical measure of customer satisfaction yet. IIS understands surveys which includes a privacy satisfaction question have recently been sent out to users to obtain their feedback on the DDL.

As an ongoing practice, it is important for the JVO and Service Victoria develop a mechanism to continue to monitor customer feedback during the state-wide rollout. Customer feedback will assist the agencies in its continuous improvement work for the DDL.

Please also see [Section 5.3.2.2](#) where we discuss fraudulent use cases and the importance of communications as a control measure.

---

<sup>8</sup> <https://www.vicroads.vic.gov.au/licences/digital-driver-licence/register> viewed 11 June 2023.

### Recommendation A – Ensure DDL communications, including privacy and security information, are accurate, consistent and fit-for-purpose

Ensure that communication for the DDL:

- Provide clear information about the differences between the JVO and the Service Victoria apps, in particular what information is shared with verifiers and whether or not an Internet connection is needed.
- Provide clear information about how to use the DDL and verify a DDL.
- Make clear that customers are not required to hand over their devices to law enforcement or other verifiers.
- Provide accurate advice about whether a plastic licence must be carried and the circumstances in which a plastic card might still need to be shown,
- Ensure messages are consistent and comprehensive across all channels and between Service Victoria, the DTP and the JVO where relevant.
- Ensure that FAQs are easily accessible, updated when necessary and cover privacy questions including potential security risks and the role and the process for checkers.

**Who:** Service Victoria and DTP

**Timeframe:** For state-wide release and ongoing

**Retained from previous PIA**

### Recommendation B – Continue to engage with businesses during state-wide release

Continue to engage with businesses to better understand their pain points and needs, as well as educating them about the licence verification process.

**Who:** Service Victoria, DTP and JVO

**Timeframe:** For state-wide release and ongoing

### Recommendation C – Continue to monitor customer feedback

Develop a mechanism to continue monitoring customer feedback (including on privacy matters) during the state-wide rollout.

**Who:** Service Victoria, DTP and JVO

**Timeframe:** For state-wide release and ongoing

## Status of recommendation from previous PIA

IIS notes the following recommendation has been implemented.

### Recommendation 4 – Include privacy in pilot evaluation

Include privacy 'satisfaction' in the evaluation of pilot communications. Issues to consider could include understanding of the QR code content, whether customers had sufficient information to make an informed choice about using a DDL, and if they were confident that privacy and security would be protected.

**Who:** DTP

**Timeframe:** For pilot

**Status:** Implemented

### 5.1.2 Disclosure

IPP 2 states that personal information may only be disclosed for the primary purpose for which the information was collected. Under OVIC Guidance, it is considered a disclosure when others are allowed to view personal information even though it remains in the possession or control of its original collector. In this instance, we are discussing the scenario where licence information on the DDL is being disclosed to licence checkers which meets the primary purpose test of IPP 2.

During the period of preparing this PIA, IIS understands there has been significant discussion between DTP, Service Victoria and JVO regarding the amount and kinds of information that should be disclosed.

For Service Victoria's DDL, based on the pilot solution, the amount of personal information disclosed to licence checkers depends on the specific use case. For example, if a customer is asked to verify their licence and the specific QR code for this is scanned, what appears on the verifier's screen is the exact same information that exists on the customer's screen – this includes the customer's name, date of birth, address, licence number, type and expiry.

This is different to JVO's approach which opted for minimal information being displayed on the checker side. For the pilot, when a verifier scans the QR code or bar code for the driver licence view, the verifier will only see the licence numbers as well as the green tick and message that the licence is verified. Customers may also choose to allow a verifier to see, and take notes of, the information on their device.

IIS understands the DTP has made a policy decision in regard to the above matter, taking into account trade-offs between usability and privacy. The DTP's position is a 'middle ground' between the Service Victoria and JVO positions. The kinds of information that will be displayed on the verifier's app, upon scanning the customer's DDL QR Code, are the following:

- Verification of licence – photo, first and last name, licence status, proficiency.

- Verification of age – indication of whether the customer is over 18 (green tick for yes, red cross for no), photo.
- Verification of identity – photo, first and last name, address.

IIS notes minimal information is involved in the verification of age, which is privacy positive. This would occur in the context of entering pubs and clubs, and which would pose a heightened privacy risk to patrons if more of the person's information was to be revealed (e.g., to an unscrupulous bouncer).

IIS understands the inclusion of the photo as part of the information being displayed to verifiers is a mitigation against spoofing of the DDL (i.e., where a person alters the appearance of the credential on a jailbroken phone). In such scenarios, the verification process may return a correct verified status even though the DDL has been tampered with; the correct customer photo that is displayed to the verifier would enable them to identify that the person has changed the photo on their side.

Overall, IIS considers the information proposed to be disclosed on the verifier side is appropriately limited to the verification use case and that the DTP has achieved a good balance between usability and privacy.

Additionally, as part of our discussion with the DTP, Service Victoria and JVO, it was acknowledged that there continues to be a need for certain businesses to retain some or all licence information as part of their legislative or operational requirements.

We note certain matters such as policy decisions, privacy decisions, and product design will require further consideration to address these requirements in the context of the DDL. It is beyond the scope of this PIA to assess these issues. However, IIS cautions against conflating the time-limited sharing of personal information for DDL verification purposes with the broader sharing (and subsequent collection) of such information for business retention purposes.

### 5.1.3 Security – IPP 4

IPP 4 requires agencies to take reasonable steps to protect the personal information they hold from misuse and loss and from unauthorised access, modification or disclosure. The DTP and Service Victoria will also be subject to the VPDSF and VPDS. The VPDS prescribes a minimum set of mandatory requirements across all security areas including governance, information, personnel, ICT and physical security. The VPDSF provides direction to Victorian public sector agencies or bodies on their data security obligations.

IIS notes the DTP treats disclosure of R&L data to Service Victoria as though it were a disclosure to a third party; its security due diligence measures take account of this context.



Business Impact Levels (BIL) are used to determine the security value of public sector information. BILs describe the potential harm or damage to government operations, organisations or individuals if there were a compromise to the confidentiality, integrity or availability of public sector information. The DTP has undertaken an Information Value Assessment (IVA) [redacted]

[redacted]

[redacted]

Factors taken into account include that:

- The DTP is sharing images and R&L data together, which it would usually only do in limited circumstances because of the sensitivity and high value of the data.
- The potential volume of data to be shared with Service Victoria.
- The impact on public confidence and community safety if the integrity of drivers licence is impacted.

IIS has not validated this assessment as part of the PIA but has not noted any issues.

#### 5.1.3.1 System security

[redacted]

Both Service Victoria and the DTP have noted a number of design features for the project that aim to mitigate the risks. Both also outlined their security approaches and noted specific steps they have taken to identify and manage security risks for the project. IIS notes that the completion of the IVA and agreement on the data classification was crucial in preparation for the regional pilot. We understand that as Service Victoria, the DTP and the IVO continue to gather feedback about the DDL, they will also continue to monitor and assess the systems and processes to ensure that it remains efficient and secure.

Security actions that are relevant for this PIA include:

- **Incorporation of Security by Design in the development of the DDL**

[redacted]

30(1), 34(1)(b), 34(4)(a)(ii)

- **Security assessments**

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Although IIS has not done a security assessment, we consider the security approach for the Service Victoria app is likely to limit both privacy and security risks. We have not identified any issues of concern.

### Status of recommendation from previous PIA

#### Recommendation 5 – Continue to monitor, assess and update privacy risks in risk register

Include privacy risks to individuals using a DDL in the risk register and ensure that these risks are continuously monitored.

**Who:** Both Service Victoria and DTP

**Timeframe:** For pilot and ongoing

**Status:** Implemented

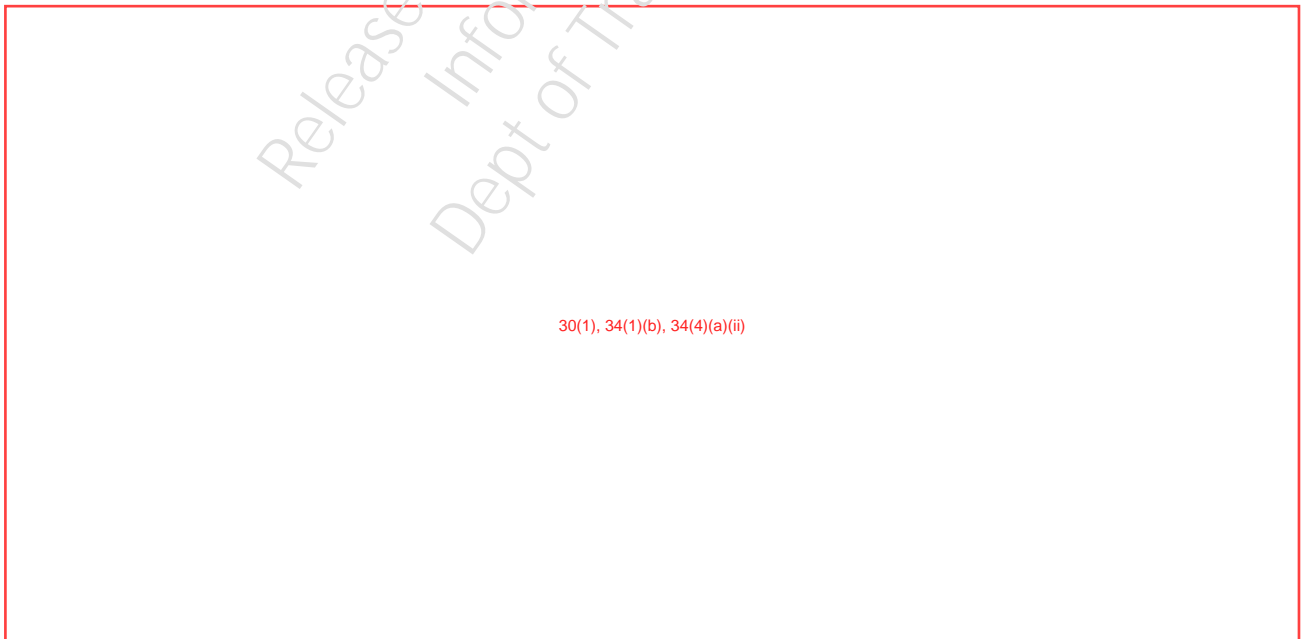
#### 5.1.3.2 Security for users of the DDL

30(1), 34(1)(b), 34(4)(a)(ii)

IIS agrees that a number of features of the Service Victoria DDL appear to offer security advantages, over and above that of a plastic licence. These include:



- A user's unique card number on the DDL is hidden by default.



30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

IIS understands that the DTP has clarified that customers are not required to hand their devices to law enforcement officials or others. This has been included in current communications and will continue to be included in future communications. IIS appreciates this measure and also encourages the DTP to explore if other measures, including legislative change, are needed.

Overall, IIS has not identified any significant areas of concern from a privacy perspective with the Service Victoria's security approach for the DDL. The approach seems consistent with privacy and security by design and is positive and comprehensive. IIS understands that Service Victoria and DTP have implemented our security recommendations, noting that at the time of writing the DTP and Service Victoria are actively considering options for limiting address display. We make no further recommendations.

### Status of recommendations from previous PIA

#### Recommendation 6 – Explore options for limiting address display on the DDL default view

Explore options for allowing differential display of address on the DDL default view.

**Who:** DTP and Service Victoria

**Timeframe:** For full rollout

**Status:** Implemented

### Recommendation 7 – Document and communicate requirements for the handling of individuals devices for DDL checking

Document policy decisions that individuals must not be required to hand over their device to DDL checkers including law enforcement. Include clear information on this issue in communications for the pilot and full rollout for individuals using DDLs and for checkers including Victoria Police.

**Who:** DTP

**Timeframe:** For full rollout

**Status:** Implemented

#### 5.1.3.3 Device limitations

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

30(1), 34(1)(b), 34(4)(a)(ii)

#### 5.1.4 Access and correction – IPP 6, and privacy complaint handling

IIS understands there will be a shared responsibility between the DTP and Service Victoria to rectify issues around the DDL. The DTP will be responsible for providing the licence information and related information about its validity, while Service Victoria will also need to field queries as the DDL will be on the Service Victoria wallet.

The MoU includes complaint handling principles to which the DTP and Service Victoria must adhere. It specifies that both parties will assist each other and cooperate to resolve any complaints or issues and that complaints will be referred to the responsible party.<sup>9</sup> IIS understands that Service Victoria has extensive experience in managing customer services issues and complaints on behalf of its agency partners, including the DTP, in accordance with its Complaint Handling Policy.

While IIS acknowledges this is not a new issue for Service Victoria, we encourage the DTP and Service Victoria to ensure there is a streamlined 'no wrong door' approach to receiving, and assisting individuals with, privacy queries and complaints related to DDL. At the time of writing the PIA, the materials for privacy complaint handling were still being developed.

Overall, IIS considers Service Victoria and the DTP have strong existing measures in place to deal with privacy enquiries and complaints. Documenting and ensuring staff awareness around the specific measures for DDL enquiries and complaints should be a priority. We also encourage Service Victoria and DTP to continue monitoring the procedures to ensure that they stay fit for purpose.

Additionally, it may be worthwhile for Service Victoria to engage with the DTP's Vulnerable Customers Team as part of its escalation processes when interacting with DDL customers who may be dealing with a 30(1), 34(1)(b), 34(4)(a)(ii). The DTP Vulnerable Customer's Team assist clients that are affected by family violence with their registration and licensing requirements, which includes changing number plate and licences due to family violence. As such, this channel may be better to deal with any enquiries or issues raised by Service Victoria customers in regard to the DDL. Possible options include an in-app function or for a pathway to be promoted on both the Service Victoria and JVO websites.

#### Recommendation D – Implement pathway to DTP Vulnerable Customers Team as part of enquiries and/or complaint handling process

Implement pathway or escalation process to DTP's Vulnerable Customers Team when interacting with DDL customers who may be experiencing a 30(1), 34(1)(b), 34(4)(a)(ii).

**Who:** Service Victoria

**Timeframe:** For state-wide release and ongoing

<sup>9</sup> Section 8.3 of MoU – Complaint Handling Principles.

## 5.2 Governance

### 5.2.1 Project governance

The DDL Project is now moving to its state-wide implementation phase. IIS has been impressed with the emphasis to date on both privacy and security by design in the design and built phases of the DDL. Strong privacy and security protective measures have been included. IIS understands that as long as the project is under 'Delivery' mode, project governance (including in relation to privacy) will be led by the Steering Committee.

IIS notes the overarching MoU has now been signed. Detailed agreements, including the DDL transaction journey and the IPA that sets out the arrangements between the DTP and Service Victoria have also been agreed on. IIS also acknowledges the collaborative relationship between the DTP, JVO and Service Victoria throughout the development of the DDLs, external pilot and the continuous efforts to ensure effective project governance, including on privacy matters. In light of this, IIS finds that the following recommendation has been met.

#### Status of recommendations from previous PIA

##### Recommendation 8 – Ensure project governance arrangements include clear privacy roles and responsibilities, including for monitoring privacy outcomes

Ensure and document a privacy approach that makes clear who is responsible for privacy sign-off for the project, and that monitoring privacy outcomes is included in its project implementation and evaluation plans.

Ensure detailed agreements and ongoing project governance processes include clear privacy requirements and responsibilities for the project, and a comprehensive and coordinated approach to ensuring privacy objectives are met.

**Who:** Service Victoria and DTP

**Timeframe:** For state-wide release and ongoing

**Status:** **Implemented**

### 5.2.2 Privacy by Design and future developments

Privacy by Design (PbD) has been a feature of the DDL project development to-date. It has been driven by Service Victoria's customer first focus, recent data breaches and the ISO standard. In stakeholder consultations, Service Victoria demonstrated that privacy remain key consideration of DDL design and development. IIS encourages both Service Victoria and the DTP to continue this approach. It will remain relevant as the DDL is implemented and further enhancements are introduced.



Particular areas for future privacy focus include:

- If a notifications feature is introduced, allowing, to the extent possible, for individual choice about whether or not to receive notifications.
- The possible display of licence status and demerit points. Both require further in-depth analysis around policy implications of formal notices/notifications in a digital environment. Where possible, individual choice should also be a key consideration.
- Interoperability with other DDLs, including scanning QR codes without needing the Service Victoria app.
- DDLs available for learners and probationary permits.
- Potential for further privacy features, for example, a record on individuals' devices of which checkers have viewed their licence.

IIS makes no further recommendations.

### Status of recommendation from previous PiA

Recommendation 9 – Continue to adopt PbD in the DDL's further development
<p>Continue the current PbD approach for the DDL, including by conducting further PIAs before making changes to the DDL, for example notifications, or display of status or demerit points, which could impact on individuals' privacy.</p> <p><b>Who:</b> Both Service Victoria and DTP</p> <p><b>Timeframe:</b> Ongoing</p> <p><b>Status:</b> Implemented</p>

### 5.3 Additional considerations – negative use cases

The assessment of privacy risks and identity theft/fraud risks have been specifically considered in this PIA by reference to use cases concerning 30(1), 34(1)(b), 34(4)(a)(ii) and fraud.

#### 5.3.1

30(1), 34(1)(b), 34(4)(a)(ii)

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

---

<sup>10</sup> See Queensland Government, 'Digital Licence app—Privacy Impact Assessment' (11 May 202), available at <https://www.publications.qld.gov.au/dataset/digital-licence-app/resource/0deb78d2-ce66-4ab3-9a28-76c77360e568>, especially Recommendation 3.

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

30(1), 34(1)(b), 34(1)(a)(ii)

30(1), 34(1)(b), 34(4)(a)(ii)

### 5.3.2 Fraudulent use cases

30(1), 34(1)(b), 34(4)(a)(ii)

30(1), 34(1)(b), 34(4)(i)(ii)

On balance, the risks of fraudulent activity exist for both the DDL and physical licence cards. Overall, IIS considers the potential for misuse by bad actors to create a false DDL credential is mitigated to a significant extent by the DDL controls including, for example, real time validation and the capacity to respond quickly to identified security issues. These are real advantages compared to the status quo of physical cards, which have their own risks with fraudulent use cases.

30(1), 34(1)(b), 34(4)(a)(ii)

## 6. Appendix A – Methodology

### 6.1 PIA approach

IIS took the following steps to carry out the PIA:

- *Planning* with the DTP and Service Victoria to confirm the approach, scope and deliverables of the PIA
- *Gathering information* by reading documents and meeting with personnel from the DTP and Service Victoria
- *Analysing the information* against privacy obligations and taking account of possible broader privacy issues, regulator guidance, and privacy good practice
- *Identifying privacy risks* and developing ways to mitigate those risks
- *Drafting the PIA report* – in this case, updating the June 2023 PIA report in relevant places, and providing this to the DTP and Service Victoria for comment
- *Finalising the PIA report* following feedback from the DTP and Service Victoria.

### 6.2 Documents reviewed

Documents reviewed
<b>DTP documents</b>
1. 230428 digital driver licence communication and engagement plan – v6 final
2. DDL DRAFT Design Standards 20230601 V.03
3. DDL Policy Standards V1.0
4. DTP Risk Matrix
5. IVA DDL 2023 both products
6. IVA DDL 2023 Final
7. Victorian Government Gazette, No. S 523, October 2022, application of PDPA to JVO
8. DDL_Design Standards_November 2023 Update - Final
9. V18 - Digital Drivers Licence (incl L's & P's) Wireframes (Nov 2023 Update)
10. V29 - QR Code Verification Wireframes (Nov 2023 Update)

## Documents reviewed

### Service Victoria documents

11. Draft Privacy Collection Notice for Digital Driver Licence – 20220504
12. Digital Driver Licence - Transaction Journey (2022.05.16)
13. Operating Service Commitment – Final
14. 221212 LOA assessment – DDL Pilot (final signed)
15. DDL DoT API Agreement for Service Victoria 20221209 V1.8 - Final
16. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
17. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
18. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
19. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
20. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
21. Service Victoria DTP DDL OVIC 040423
22. Service Victoria [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii) assessment
23. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
24. [Redacted] 30(1), 34(1)(b), 34(4)(a)(ii)
25. Service Victoria Collection Notice <https://service.vic.gov.au/digital-driver-licence-privacy-collection-notice>
26. Service Victoria Privacy Policy <https://service.vic.gov.au/privacy-and-security>
27. Service Victoria 'How to Guide for Licence Checkers'
28. Service Victoria DDL page - <https://service.vic.gov.au/find-services/digital-wallet/digital-driver-licence/checking-digital-driver-licences>



### 6.3 Meetings held

Meetings held	Date
Pre kick-off meeting <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● DTP personnel</li> </ul>	10 October 2023
Kick-off meeting with Service Victoria <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● Service Victoria personnel</li> </ul>	11 October 2023
PIA information gathering meeting – Product Team and IT/Security <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● Service Victoria personnel</li> </ul>	30 October 2023
PIA information gathering meeting – Vulnerable Customers Team (DTP) <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● DTP personnel</li> </ul>	31 October 2023
PIA information gathering meeting – Policy, Legal and Comms <ul style="list-style-type: none"> <li>● IIS personnel</li> <li>● Service Victoria personnel</li> </ul>	2 November 2023

## 7. Appendix B – Assessment against the IPPs

The following table sets out IIS’s high-level assessment Service Victoria DDL against the IPPs in the context of the expected state-wide full release in December 2023.

30(1), 34(1)(b), 34(4)(a)(ii) This will include some health information in form of licence codes. This would be subject to the HPPs in the HRA. IIS notes that the HPPs cover similar issues to the IPPs.

IIS notes that when Service Victoria is collecting data in the context of the DDL, for example, to validate a licence, it is doing so on behalf of the DTP. However, the DTP treats disclosure of R&L data as though it is a disclosure to a third party.

IIS also notes that where our assessment has not identified specific issues for this PIA, that is not meant to indicate there is no privacy work to be done. IIS anticipates that usual privacy compliance and monitoring would occur.

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 1 – Collection</b></p> <p>An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation’s Privacy Policy.</p>	<p>The DDL involves a re-use of existing information the DTP holds, not a new collection for the DTP.</p> <p>The MoU specifies that Service Victoria will be collecting personal information on behalf of the DTP (in the process of loading DDL into the Service Victoria wallet, and in the process of creating/refreshing QR codes).</p> <p>The introduction of DDL is a new way of providing driver licences and as such privacy policies and collection notices are to be updated to reflect the changes.</p> <p>See discussion at <a href="#">Section 5.1.1</a>.</p>

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 2 – Use and disclosure</b></p> <p>Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual's consent, for a law enforcement purpose, or to protect the safety of an individual or the public.</p>	<p>The DTP's use of R&amp;L data for digital driver licence is consistent with the purpose of collection.</p> <p>The IPA also specifically states that Service Victoria undertakes that information shared by the DTP will only be used and disclosed for the purposes set out in the IPA (To provide an alternative digital customer channel for some vehicle registration and driver licensing activities and services of the Department of Transport including under the RSA). Section 90K of Part 7B of the RSA sets out the authorised use or disclosure. Section 90K(a)(vi) allows disclosure in relation to an intergovernmental agreement.</p> <p>See additional discussion of disclosure in the context of QR code verification at <a href="#">Section 5.1.2</a>.</p> <p>Overall, IIS considers that the information proposed to be disclosed on the verifier side is appropriately limited to the verification use case and that the DTP has achieved a good balance between usability and privacy.</p>
<p><b>IPP 3 – Data quality</b></p> <p>Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.</p>	<p>The DDL should not diminish and may enhance data accuracy of driver licence information.</p> <p>Changes to driver licence details or status will be subject to pilots and roll-out and will be reflected in the DDL quickly.</p> <p>Service Victoria's design of the DDL is in such a way that it does not collect or hold identified personal information except in the limited context of the generation of the QR code. The one source of truth of driver licence information remains with the DTP.</p> <div data-bbox="778 1682 1398 1765" style="border: 1px solid red; padding: 5px; text-align: center;"> <p>30(1), 34(1)(b), 34(4)(a)(ii)</p> </div> <p>No issues identified.</p>

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 4 – Data security</b></p> <p>Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.</p>	<p>The DTP and Service Victoria have in place detailed security management processes and have commenced or undertaken detailed security risk assessments for the DDL.</p> <p>See further discussion at <a href="#">Section 5.1.3</a>.</p>
<p><b>IPP 5 – Openness</b></p> <p>Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation’s Privacy Policy.</p>	<p>Service Victoria has updated its privacy policy containing a specific section on the DDL. The intention is that the materials will be consistent and that individuals are easily able find relevant information to inform their decisions.</p> <p>See further discussion regarding transparency and public communications at <a href="#">Section 5.1.1</a>.</p>
<p><b>IPP 6 – Access and correction</b></p> <p>Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982 (Vic).</p>	<p>The introduction of the DDL should not affect current processes for access and correction. However, Service Victoria and the DTP should ensure respective responsibilities are clear and that processes are built with a ‘no wrong door’ approach.</p> <p>See further discussion at <a href="#">Section 5.1.4</a>.</p>
<p><b>IPP 7 – Unique identifiers</b></p> <p>A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.</p>	<p>Driver licence numbers are unique identifiers in terms of the PDPA.</p> <p>Driver licence numbers will appear on the DDL. However, the DDL project does not involve the assignment of new unique identifiers.</p> <p>No issues identified.</p>

Summary of privacy principle	High level assessment against IPPs for DDL project for Service Victoria and DTP
<p><b>IPP 8 – Anonymity</b></p> <p>Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.</p>	<p>Not relevant for the DDL – identification is a required part of acquiring or using a DDL.</p>
<p><b>IPP 9 – Transborder data flows</b></p> <p>If an individual’s personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.</p>	<p>IIS understands that Service Victoria uses <span style="border: 1px solid red; padding: 2px;">34(1)(b), 34(4)</span> physically located in the Sydney region. Service Victoria maintains control over the data and NSW has a privacy legal regime that is substantially similar to the Victorian IPPs. IIS is not aware of any legal issues with this arrangement.</p> <p>No issues identified</p>
<p><b>IPP 10 – Sensitive information</b></p> <p>The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.</p>	<p>Driver licence processes do not involve the collection of sensitive information as defined, but do involve some biometric and health information (See <a href="#">Section 3.6.2</a>). Such information is part of the R&amp;L data that the DTP has already collected.</p> <p>No issues identified.</p>

Released under the Freedom of  
Information Act 1982  
Dept of Transport & Planning

INFORMATION INTEGRITY SOLUTIONS PTY LTD

PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438

F: +61 2 9319 5754

E: [contact@iispartners.com](mailto:contact@iispartners.com)

[www.iispartners.com](http://www.iispartners.com)

ABN 78 107 611 898

ACN 107 611 898



**IIS Partners**  
INFORMATION INTEGRITY SOLUTIONS