DIGITAL LICENCE APP
PRIVACY IMPACT ASSESSMENT

April 2020

Executive summary

Crown Law has been engaged by TMR to undertake a PIA for the Digital Licence App to:

- identify, analyse and define the major privacy impacts arising from the Digital Licence App; and
- make recommendations and identify strategies to comply with privacy requirements.

The Digital Licence App is a mobile application that will allow users to securely store credentials issued by the Queensland Government in a digital format. It is intended to give Customers control over their stored credentials, provide access to a range of government services and allow Customers the capability to pay for services and other products electronically.

An initial PIA was completed for the Digital Licence App in August 2019 when it was in the early stages of development with the intention of updating the PIA, or undertaking additional PIAs, as the Digital Licence App was further developed. The initial rollout of the Digital Licence App will have limited functionality, including learner, provisional and open driver licences, marine licences and photo identification cards. However, it is anticipated that future functionality may extend to additional TMR documents and credentials issued by other government agencies.

The scope of the original PIA was undertaken prior to a vendor having been contracted to deliver the App. It was therefore limited to the initial proposed functionality of the Digital Licence App and the information then available as to the architecture of the Digital Licence App. Now that a vendor, Thales, has been contracted, this updated PIA considers more detailed architecture of the Digital Licence App, including security features. It also includes the development of a Reader App to be used by Verifiers to scan or 'read' Digital Licences provided by Customers.

The following table sets out key privacy risks, recommendations to address those risks and the priorities for the measures and recommendations:

Privacy risks	Recommendations	Priority
1. Misunderstanding by individuals about why their personal information is being collected and how it will be used	Inclusion of a detailed privacy notice and consent at the time a Customer applies for a Digital Licence and when the Customer downloads the Digital Licence App. The privacy notice should be drafted specifically for the Digital Licence App and users should not be directed to general privacy policies or statements. Recommendations 1, 4 and 7	High

2.	Privacy notices are not provided consistently across all communication channels, leading to confusion	Ensure that the same privacy notice and consent is provided to Customers irrespective of the method they use to apply for a Digital Licence and when they access the Digital Licence App. Recommendations 1 and 4	High
3.	Misuse or inappropriate disclosure of user's personal information	Implementation of strict security and access procedures Obtaining privacy consents from Customers Ensuring arrangements with contractors impose appropriate security requirements and controls over personal information Recommendations 1, 5 and 6	High
4.	Use of personal information that is inaccurate, not up to date or incomplete.	Implementing a prompt in the Digital Licence App that reminds Customers to update their personal information regularly Recommendations 2 and 3	Moderate
5.	Function creep	That further privacy impact assessments be carried out before any additional functions are added to the Digital Licence App or Reader App. Additional functionality includes: • addition of credentials to the Digital Licence App; • expansion of tasks or activities to be performed in the Digital Licence App or Reader App; • changes to the way personal information is collected, stored, used or disclosed in conjunction with the Digital Licence App or Reader App; and • collaboration with other government agencies Recommendations 7 and 8	Future

Glossary

Customer	A person who applies for, and is granted access to, the Digital Licence App
Digital Licence	A digital copy of a Customer's Driver Licence, Photo Identification Card or Marine Licence that is stored in the Digital Licence App
Digital Licence App	A mobile application that allows users to have online access to their Digital Licence credentials. The Digital Licence App may be supported by a website where users can apply for a Digital Licence and access their Digital Licence App account. The Digital Licence App will also include functionality that allows a user to verify another Customer's Digital Licence in a similar way to the Reader App.
Driver Licence	A learner, provisional or open licence to drive a C class vehicle issued under the Driver Licensing Regulation
Driver Licensing Regulation	*Transport Operations (Road Use Management – Driver Licensing) Regulation 2010*
IPP	Information Privacy Principle
IP ACT	*Information Privacy Act 2009* (Qld)
IP Guidelines	The *Guidelines – Privacy Principles* published by the Queensland Information Commissioner
ISO 18013	ISO/IEC 18013-5: Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application
Marine Licence	A recreational marine licence issued under the *Transport Operations (Marine Safety) Regulation 2016*
Marine Safety Act	*Transport Operations (Marine Safety) Act 1994*
Marine Safety Regulation	*Transport Operations (Marine Safety) Regulation 2016*
Photo Identification Card	A photo identification card issued under the PIC Act

PIA	Privacy Impact Assessment
PIC Act	*Photo Identification Card Act 2008*
Reader App	A standalone mobile application that can be used to scan and validate the authenticity of a Digital Licence presented by a Customer
TMR	Department of Transport and Main Roads
TORUM	*Transport Operations (Road Use Management) Act 1995*
TRAILS	The Transport Registration and Integrated Licensing System operated by TMR containing information about its customers
Verifier	An entity or person that uses the Digital Licence App or a Reader App for the purpose of verifying the Digital Licence of a Customer. Verifiers are also known as Credential Users within the context of ISO18013-5.

Table of contents

1. Introduction

1.1 What is a privacy impact assessment?

A PIA is an assessment of the possible privacy impacts of a project. It identifies privacy risks and options for managing, minimising or eliminating those risks.[1]

1.2 Scope of this PIA

Crown Law has been requested to carry out a PIA to:

- ensure that the major privacy impacts arising from the Digital Licence App are identified, analysed and satisfactorily defined in accordance with the IP Act; and
- identify recommendations and strategies to meet privacy requirements in sufficient detail to enable adoption within the detailed design, build, deployment and on-going operation of the Digital Licence App.

The scope of this PIA does not include analysis of privacy impacts relating to:

- any Digital Licence App or Reader App dependency elements, such as TRAILS, Oracle or any associated identity verification system that is used for verifying a Customer's identity;
- integration with other systems, such as Q-Lite;
- development of an Identity Service Provider service by TMR in conjunction with development of the Digital Licence App;
- the privacy obligations of Verifiers or other third parties;
- analysis of privacy requirements other than those applying in Queensland;
- analysis of business processes beyond those impacted by the implementation of the Digital Licence App;
- any potential or unconfirmed perceived risks; and
- community consultation.

This PIA is based on a review of the material available and the law in force as at April 2020 and discussions with TMR officers. It is also limited in scope to the initial proposed functionality of the Digital Licence App and Reader App, as discussed at sections 2.4 and 3.2.

[1] See page 1 of the Office of the Australian Privacy Commissioner, *Privacy Impact Assessment Guide*, May 2014, which is available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide.

1.3 Methodology

The methodology is generally based on the methodology set out in the Office of the Information Commissioner's *Privacy Impact Assessment (PIA) Guideline*.[2]

The stages in conducting the PIA were as follows:

Project description **-** This stage involved broadly describing the Digital Licence App as set out in section 2.

Mapping the information flows **-** This involved obtaining detailed information about the information flows and describing those flows in section 5.

Privacy impact analysis **-** This stage involved analysing how the Digital Licence App program impacts on privacy. The analysis is set out in section 6.

Privacy management and recommendations **-** This involved considering the results of the privacy impact analysis, developing recommendations and producing this report.

[2] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment.

2. Overview of Digital Licence App

2.1 Background and context

The Queensland Government has issued Driver Licences since 1910.

TMR currently issues Driver Licences, Marine Licences and Photo Identification Cards as well as a range of transport related licences, accreditations, certificates or authorisations to appropriately qualified people. Driver Licences and Photo Identification Cards are a primary form of identification in Queensland.

Driver Licences, Marine Licences and Photo Identification Cards are currently issued as a physical smartcard or endorsement on a physical smartcard. The physical cards are used to demonstrate a person's authority to do particular transport activities or as evidence of age (for a variety of purposes) and may also be used for law enforcement purposes.

The Digital Licence App is the next evolution of licensing and identification products that align with the increasing preference of TMR's customers for mobile digital services. It will display the near real time status of the product and include security features that will allow users to confirm its validity as well as allowing the Customer to control what information is displayed.

2.2 Digital Licence App

The Digital Licence App is a mobile application that allows access to Customer's digital credentials and enables digital transactions through a mobile device.

Physical credentials will still be issued by TMR and Customers may have physical and digital credentials concurrently. The information contained in the Digital Licence App will generally reflect the information contained in the Customer's physical credential, but may also contain additional information. For example, it may include dynamic updates to show the current status of the credentials (e.g. whether it is suspended or cancelled). It will also allow Customers to update their personal information.

The Digital Licence App will access information from TRAILS through an encrypted and secure connection to the mobile device. The Information and Communications Technology (ICT) contractor engaged to build and manage the Digital Licence App will not store or access any unencrypted personal information from TRAILS.

Information from TRAILS will be encrypted before it is transferred to the Digital Licence App. In so far as the relevant ICT contractor 'touches' that information during the transfer between TRAILS and the Digital Licence App, it will not be able to view the personal information.

Once the encrypted data is received by the Digital Licence App, the particular encryption that is known only to the app, will unencrypt the data at the time it is displayed on the Customer's mobile device.

Personal information about a Customer and their digital credentials will be cached locally in their mobile device. When the Customer accesses the Digital Licence App, it will display a cached copy of the last updated information.

The information flows involved in a Customer's use of the Digital Licence App largely reflect the existing process for hardcopy smartcards. Limited additional collections, uses and disclosures of personal information will occur as a result of a Customer applying for, and using, a Digital Licence.

The Digital Licence App will change the way in which Customer's may choose to disclose their personal information to third parties. A significant difference is that Customers can choose to allow third parties to only access part of the information contained in a credential. For example, a Customer may choose to limit the data a person sees to just their photo and confirmation that they are over 18 years of age. The third party would not see their name, address, medical condition or date of birth. This will provide a considerable benefit to the Customer, allowing them control over privacy decisions. It is proposed that third parties will be able to validate the Digital Licence presented by a Customer by using a QR code, or similar, that is scanned by a device operated by the third party using the Reader App or the Digital Licence App.

The Customer will be able to view a data access log that shows who has accessed data in their Digital Licence. That data access log will be stored on the Customer's mobile device and will not be accessed by TMR.

Customers will be given a prompt before they provide their Digital Licence App to a Verifier. The prompt will expressly inform Customers that presenting their mobile device to a Verifier for verification will result in their personal information being disclosed to that Verifier. A description of the personal information to be shared will also be included in the prompt.

Importantly, Customers will not be required to have a Digital Licence. Physical credentials will still be available. Even if a Customer obtains a Digital Licence, they will still have a hardcopy credential that can be used. That is, even if a Customer applies for a Digital Licence, they can choose not to use it in particular circumstances and instead rely on their hardcopy credential.

2.3 Access to the Digital Licence App

The process for Customers to apply for and access the Digital Licence App will involve an identity verification process that results in a unique code or password being issued to the Customer. The steps for a Customer to access the Digital Licence App are:

- The Customer will download the Digital Licence App from their preferred App store;

- The Customer will then enter in their CRN;
- The CRN is then validated to determine if the Customer has an Auth0 account;
- The Customer then enters their name, date of birth, postcode, mobile phone number and email address which are validated by Auth0;
- The Customer then creates their Auth0 password;
- A one-time-password is then issued to the mobile phone number recorded;
- The Customer then creates their six-digit PIN (This 6-digit PIN is in addition to any device-based security, such as a numeric or biometric PIN to unlock the mobile device).
- Once this has occurred the Customer will be able to access their digital credentials in the Digital Licence App.

2.4 Initial scope of the Digital Licence App

The Digital Licence App has been developed as a Minimum Viable Product (MVP) for a restricted public pilot. The MVP will be further elaborated based on feedback from pilot participants and Government priorities. TMR then intends to rollout further improvements to the Digital Licence App to include additional features, credentials and functionality.

It is proposed that the Digital Licence App will be piloted on the Fraser Coast (Maryborough and Hervey Bay) commencing in the first half of 2020.

This initial PIA has been completed on the basis that the Digital Licence App will commence initially with Driver Licences (learner, provisional and potentially open), Marine Licences and Photo Identification Cards with the following functionality:

- Customers can change their contact details through the Digital Licence App;
- TMR is able to send push notifications to Customers through the Digital Licence App; and
- the ability for a Verifier to validate a Digital Licence within the Digital Licence App upon production by the Customer by scanning with the Reader App or another Digital Licence App.

2.5 Future development of the Digital Licence App

It is envisioned the Digital Licence App will eventually support:

- all TMR issued smartcard products;
- the ability for TMR and other Queensland Government entities to directly communicate with Customers;

- secure digital authentication to ensure the privacy of Customers;
- visibility and management of additional products such as vehicle and vessel registrations;
- easy payments and transactions such as vehicle/vessel registration and licence/authority renewals; and
- the potential to include other government authorisations (for example, Blue Cards, Fishing Licences, High Risk Work Licences, Responsible Service of Alcohol Certification and/or Camping Permits).

Further privacy impact assessments will need to be undertaken as this additional functionality is rolled out.

2.6 Security of the Digital Licence App

The Digital Licence App is being developed on the basis of the following principles.

The Digital Licence App will include security features to ensure the Customer's data is protected against cybercrimes and theft. Verifiers will have confidence that the Customer is providing a legitimate and reliable form of identification.

This includes having the ability to verify that the credential is not a "screen shot" by requiring a credential to be verified by firstly performing "device engagement" by scanning a QR code or NFC through the Reader App or another Digital Licence App which then performs "data retrieval" offline using Bluetooth low energy or NFC or online using secure APIs back to the Issuing Authority. Further, the Digital Licence App will include a clear statement regarding the last time the credential was updated.

The Digital Licence App will give the Customer control about how much information they share with others. The Customer user will determine the information they want to display. For example, if they want to prove their age, the credential will allow the Verifier to see their photo and confirm that they are at least 18 years of age. The person needing to sight their age does not need to see the Digital Licence holder's name, date of birth, or where they live. Customers will be prompted by the app before they provide their credential for verification by a Verifier.

Security features will be applied to digital products to deter development of fraudulent products and the fraudulent use of authentic products. Digital products will:

- have the last date the information was updated displayed,
- have on screen digital security features,
- be able to be wirelessly authenticated/verified by a complementary receiving 'app', and
- have features that protect the information, including personal information, stored in the app and safeguard the link to TMR's database.

Customers will be able to see within the Digital Licence App a log of information that they have shared with Verifiers at a particular date and time. Customers can turn the audit log off or delete the audit log. TMR cannot see the audit log because it is local to the device the Digital Licence App is loaded on.

Other security features regarding storage of data and integration with TRAILS is set out in section 6.4 of this PIA. In particular, the transfer of information from TRAILS to the Digital Licence App will only involve encrypted data.

2.7 Staff portal

TMR staff will have access to a portal from which they can administer the Digital Licence App accounts of Customers. The staff portal will allow TMR to:

- search for Customers using the Digital Licence App and display their information;
- revoke access to a Digital Licence and re-instate a Digital Licence;
- control login and access; and
- review user history (but not track a user's movements or where they have verified their App).

3. Overview of the Reader App

3.1 Background and context

The ICT contractor engaged to develop the Digital Licence App has also been engaged by TMR to develop a Reader App. Third parties will be able to download the Reader App from the App store to enable them to validate Digital Licences offered by Customers for verification.

TMR will not collect or store any personal information from Verifiers when they download or use the Reader App. In particular, the identity of Verifiers will not be recorded or stored by TMR. Further, TMR will not use or disclose any personal information in conjunction with a Verifier's use of the Reader App. The only disclosure made by TMR in conjunction with the Reader App is a disclosure of information about a Digital Licence made with the consent of the Customer through the Digital Licence App. That disclosure is considered in the context of the Digital Licence App for the purpose of this PIA.

The functionality of the Reader App is also built into the Digital Licence App itself. As such, a Verifier may use their own Digital Licence App to verify another Customer's Digital Licence. The verification process is the same whether a Verifier uses the Digital Licence App or the Reader App.

A standalone Reader App is necessary for business where a device can be shared by several staff, rather than having to use a personal device to verify licences. The standalone Reader App means that no one has to share their personal information with other staff.

3.2 Initial scope of the Reader App

The Reader App will be able to scan and validate that a Digital Licence within the Digital Licence App is genuine. It will display information that the Customer has consented to share, through the Digital Licence App, but will not be able to store any data provided by the Customer or TMR.

Verifiers can use the Reader App to read the QR code displayed on a Customer's mobile device after the Customer has consented to share their data through the Digital Licence App. The Verifier will be able to see information displayed on their mobile device within the Reader App, but only such information that the Customer has consented to share with the Verifier. The Reader App does not store the personal information of Customer's and once the Verifier moves away from the screen, the displayed information can no longer be accessed.

It is intended that, in the future, pubs/clubs in Safe Night Precincts will also be able to scan a digital licence for the purpose of Part 6AA of the *Liquor Act 1992* (Qld). There are currently approved scanners that are used to scan physical licences at safe night precincts. The scanner software will need to be modified to support the scanning of

digital licences. TMR is working with Office of Liquor and Gaming and the approved scanning companies to ensure that scanning devices in safe night precincts will be able to scan and retrieve data that has been consented to be released by Customers. The Customer will still need to consent to share their name, date of birth and photo. The data would then be checked against the 'banned' list and stored for up to 30 days as required by law.

Verifiers will not be required to complete an authentication process when downloading the Reader App. Such functionality may be added to the Reader App in the future and Recommendation 8 of this PIA applies in regard to that additional functionality.

Initially, police will use the Reader App installed on their Q-Lite device. However, TMR intends to provide QPS with the Software Development Kit so that police can scan the Digital Licence App and populate the part of their QLite that draws data from the police QPRIME system. The operation of this app will remain consent based and will require the consent of the Customer in providing their mobile device so police can scan the QR code for verification. Police will not need to handle or touch the Customer's mobile phone to do this.

The scope of the verification function within the Digital Wallet App reflects the scope of the Reader App identified above.

3.3 Security of the Reader App

No personal information of Customers or Verifiers is stored within the Reader App.

Secure tokens are exchanged between the mobile devices of Customers and Verifiers so that the Reader App knows that the Digital Licence App presented is genuine, and it can decipher the QR code and exchange information.

When offline, the information is shared between devices using Bluetooth and TMR is not involved in that exchange of information. When the mobile devices are online, the QR code may instruct the Reader App to retrieve the data from TMR via the internet so that the information is current. As noted above in relation to the Digital Licence App, all information is encrypted in transit and at rest.

TMR will not maintain an access or audit log in relation to the Reader App. Transactions occurring between a Customer and Verifier are not recorded by TMR.

4. Privacy requirements

4.1 Legislative requirements

The most relevant legislative privacy requirements impacting on the Digital Licence App and the Reader App are the IP Act and specific confidentiality provisions in transport legislation.

The IP Act requires Queensland Government agencies to comply with the IPPs. The IPPs deal with the collection, storage, use and disclosure of personal information.

'Personal information' is defined in the IP Act section 12 of the IP Act as follows:

> ***Personal information*** is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

The transport Acts identified below contain similar confidentiality provisions that prohibit disclosure, recording and use of information except in specific circumstances.

Section 7(2) of the IP Act provides that it operates subject to the provisions of other Queensland Acts relevant to the collection, use and disclosure of personal information. Therefore, TMR must comply with both the IP Act and other legislative provisions about protection of a Customer's information.

4.2 Transport legislation

The relevant provisions in transport legislation are set out below.

Photo Identification Card Act 2008

Information contained in a Photo Identification Card is maintained in a register under section 26 of the PIC Act, which forms part of TRAILS.

Section 30 of the PIC Act sets out specific circumstances in which the chief executive may release information contained in the register. However, it does not otherwise prohibit the disclosure or use of the information contained in the register. It is a permissive, rather than prohibitive, provision.

Section 46 of the PIC Act prohibits disclosure, recording or use of information gained through administration of the Act except in limited circumstances. The relevant exceptions include where the disclosure, recording or use is:

- in the discharge of a function under the PIC Act;
- authorised under another Act or a regulation; or
- authorised by the person to whom the information relates.

Section 47A of the PIC Act allows the chief executive to keep and use information obtained under the PIC Act or transport legislation for cross-purposes. That is, information under the PIC Act can be used for a purpose associated with a transport Act and vice versa.

Information about Customers collected and used by TMR for the purpose of administering Photo Identification Card will be subject to these restrictions.

Transport Operations (Road Use Management Act)

Section 77 of TORUM sets out specific circumstances in which the chief executive may release certain personal information. However, it does not otherwise prohibit the disclosure or use of information. It is a permissive, rather than prohibitive, provision.

Section 143 of TORUM prohibits disclosure, recording or use of information gained through administration of the Act except in limited circumstances. The relevant exceptions include where the disclosure, recording or use is:

- in the discharge of a function under TORUM;
- authorised under another Act or a regulation; or
- authorised by the person to whom the information relates.

Information about Customers collected and used by TMR for the purpose of administering Driver Licences will be subject to these restrictions.

Transport Operations (Marine Safety) Act 1994

Section 63I of the Marine Safety Act is similar to section 30 of the PIC Act and section 77 of TORUM. Once again, it is a permissive, rather than prohibitive, provision.

Section 205AC of the Marine Safety Act is substantially the same as section 46 of the PIC Act and section 143 of TORUM. It prohibits disclosure, recording or use of information gained through administration of the Act except in limited circumstances. The relevant exceptions include where the disclosure, recording or use is:

- in the discharge of a function under the Marine Safety Act;
- authorised under another Act or a regulation; or
- authorised by the person to whom the information relates.

Information about Customers collected and used by TMR for the purpose of administering Marine Licences will be subject to these restrictions.

Other transport legislation

Other transport Acts contain confidentiality provisions, but are not directly related to the initial functionality of the Digital Licence App. That is because they apply to

information obtained by TMR in relation to administration of different credentials not within the initial scope.

However, many of the other confidentiality provisions are substantially the same as those discussed in this PIA. For example:

- Section 148C of *Transport Operations (Passenger Transport) Act 1994* is substantially the same as section 46 of the PIC Act and section 143 of TORUM;
- Section 36GA of the *Transport Planning and Coordination Act 1994* is substantially the same as section 46 of the PIC Act and section 143 of TORUM.

Detailed provisions about disclosure of vehicle registration information are contained in sections 112 to 118 of the *Transport Operations (Road Use Management—Vehicle Registration) Regulation 2010*. However, they operate as authorisations to release information, not a prohibition on disclosure or use of personal information.

4.3 *Transport and Other Legislation (Road Safety, Technology and Other Matters) Amendment Bill 2020*

The *Transport and Other Legislation (Road Safety, Technology and Other Matters) Amendment Bill 2020* was introduced into Parliament on 17 March 2020. It will amend the *Transport Planning and Coordination Act 1994* to include a new Part 4E that deals with digital authorities, digital evidence of age and digital evidence of identity. This new Part, when commenced, will permit individuals to prove their identity, age or provide an authority through the Digital Licence App.

The *Liquor Act 1992* will also be amended to permit the scanning of a digital authority, a digital evidence of age or digital identity instead of the scanning of a hard copy proof of age or identity document.

These provisions will facilitate the transactions proposed to be undertaken by Customers and Verifiers through the Digital Licence App and the Reader App.

4.4 Privacy guidelines

The Office of the Information Commissioner has published the IP Guidelines about the IPPs, privacy complaints and other aspects of the IP Act.[3]

[3] http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles.

5. Information flows

5.1 Existing information flows

Table 5.1 summarises the avenues and flow of communication for customer information. Consents are obtained from customers at the time of applying for a Driver Licence, Marine Licence or Photo Identification Card to allow TMR to use and disclose information in these ways.

5.2 Information flows in the Digital Licence App

The Digital Licence App does not significantly alter the existing information flows between TMR, Customers and third parties. Rather, it changes the method by which information is exchanged. The additional personal information flows involved in the Digital Licence App are detailed in Table 5.2.

5.3 Information flows in the Reader App

TMR will not collect, store, use or disclosure personal information in conjunction with the Reader App, other than to the extent information is disclosed by TMR to Verifiers with consent of the Customer. That disclosure is analysed as part of the information flows within the Digital Licence App. There are no additional information flows between TMR and third parties win the context of the Reader App.

The position is the same to the extent that a Verifier uses a Digital Licence App to verify the digital Licence of another Customer.

Table 5.1Existing information flows

Business process/activity	Components of personal information	Collection	Storage	Use	Disclosure
Application for Photo Identification Card, Driver Licence or Marine Licence	• Name • Address • Customer reference number • Date of birth • Medical conditions • Phone • Email • Previous names	Customer approaches TMR, makes application in writing or verbally and produces identification. TMR staff sights identification and checks application form.	TMR staff enter data into TRAILS.	TMR provides information to smartcard production vendor to prepare the hardcopy card. Smartcard production vendor produces the smartcard and mails it to the customer's nominated postal address. TMR staff access customer information for use in performing departmental functions, including to renew or upgrade the credential.	Dislcosures may be made by TMR for various reasons in accordance with legislative authorities in transport legislation. Customer discloses credential to third party to prove their identity or age. Third party has access to all information on the credential and may take a copy.* Customer discloses credential to police officer.* Police officer can access details from TRAILS using Q-Lite device, including traffic history. * This is a disclosure by the Customer, not TMR.
Update of information	• Name • Address • Medical conditions • Other info	Customer approaches TMR in person or online to update their details.	TMR staff enter data into TRAILS.	As above if new card required. For address changes, TMR produces label to be affixed to existing card and sends to Customer.	As above

Table 5.2 Digital Licence App information flows

Business process/activity	Components of personal information	Collection	Storage	Use	Disclosure
Application for Digital Licence	• Name • Address • Customer reference number • Date of birth • Proof of ID • Phone number • email	Customer may apply for a Digital Licence at the time of the application for a credential or at a later date. Independent ID verification service confirms identity	Data uploaded into TRAILS (if relevant) Digital Licence information stored in mobile application server	TMR provides information to Digital Licence App vendor. Data is encrypted when it leaves TRAILS and remains encrypted while being transferred to the Customer's mobile device. Digital Licence App vendor produces the credential in a secure Digital Licence App that is accessed by the Customer on their mobile device. Data is unencrypted at the point it is received on the Customer's mobile device. TMR staff access Customer information for use in performing departmental functions, including to renew or upgrade the credential.	Disclosures may be made by TMR for various reasons in accordance with legislative authorities in transport legislation, but not in the context of the Digital Licence App. TMR will disclose information to Verifiers upon authorisation by the Customer to verify their identity upon the Verifier scanning the Digital Licence. The Customer will consent to the disclosure by providing their device for scanning. The Customer may disclose information in the credential to Verifier to prove their identity or age. Where this does not involve scanning of the mobile device this will be a disclosure by the Customer, not TMR. Customers disclose credentials to police officer. Police Officer can scan Digital Licence using Q-Lite device. Police officer can access details from TRAILS using Q-Lite device, including traffic history. Police cannot access information unless authorised by law or with

					cooperation of the Customer.
Customer uses the Digital Licence App to update their details	• Name • Address • Medical conditions • Other info	Customer uses Digital Licence App to provide updated information to TMR.	TMR staff enter data into TRAILS Digital Licence information stored in mobile application server	As above	As above
Access log within Digital Licence App	• Validation date and time • List of data accessed and validated • Device receiving validation	The Digital Licence App will log the relevant information in an 'Access Log' that can be reviewed by the Customer to show usage of their Digital Licence.	Mobile application server	To display a data access log to the Customer	None No disclosures are made of access log in ordinary course of business. If police require access log, such access must be authorised under law or provided with the Customer's consent.
Security access log	• Date and time of access to Digital Licence App by Customer	The Digital Licence App will collect security audit log information routinely when used by Customer	Mobile application server	To audit access for information security purposes	None

5.4 Detailed information flows

5.4.1 Collection of personal information

The additional personal information that will be collected through the Digital Licence App is set out in the table below, along with the relevant purpose for which it is collected.

Information collected	**Purpose of collection**
Name and email address of Customer collected at time of applying for Digital Licence	To allow Customers access to the Digital Licence App
Proof of identity information required for accessing Digital Licence App (requirements yet to be confirmed)	To verify identity of user for the purpose of allowing them access to the Digital Licence App
Personal information that is uploaded to the Digital Licence App by Customers	To ensure that TMR's records about users are up to date and accurate for the purpose of administering the Digital Licence App and associated licences and authorisations
Audit log information, e.g. date and time of authentication for access to the Digital Licence App, number of devices used by a Customer, details of credentials in a Customer's Digital Licence App and when a credential is removed. Record of messages sent to the Customers through the Digital Licence App.	To audit access for information security purposes and display a data access log to the Customer To keep TMR's records about Customers up to date.
Details relating to access made by a mobile device – name of device, unique identifier and location information	To implement security safeguards by detecting unauthorised use To analyse and optimise functionality of the Digital Licence App

5.4.2 The distinction between use and disclosure

TMR will use personal information if it:

- manipulates, searches or otherwise deals with the information;
- takes the information into account in the making of a decision;

- transfers the information from a part of the entity having particular functions to a part of the entity having different functions; or
- publishes the information in a way that does not identify the individual the subject of the information.[4]

TMR will disclose personal information if it causes another entity to know, or to be able to know, the information and cannot exercise direct control over who will know the information in the future.[5]

The test for working out whether there is a use or disclosure is whether the agency maintains control over the personal information. If control is given up to another entity, it is disclosure. If the agency maintains control over the information, it is treated as use. An agency is considered to maintain control over personal information if it gives the personal information to another part of the entity with different functions.

The distinction between use and disclosure of personal information will be particularly important in relation to the engagement of ICT service providers. If TMR maintains control over personal information that is given to service providers, through binding contractual terms, then the provision of that information will constitute a use, rather than disclosure. The content of contracts with service providers is further discussed at section 6.5 of this PIA.

5.4.3 Use of personal information

This table identifies the uses of personal information that will occur in connection with the Digital Licence App.

Information used	Description of use	Purpose of use
Customer personal details that are contained in TRAILS	Information will be transferred between TRAILS and the Digital Licence App	To create and provide ongoing online access to the Digital Licence App
Customer personal details that are uploaded to the Digital Licence App by the user	Information will be transferred between the Digital Licence App and TRAILS	To create and provide ongoing online access to the Digital Licence App To allow Customers to communicate with TMR To ensure user records are kept up to date

[4] Section 23(3) of the IP Act.
[5] Section 23(2) of the IP Act.

Information used	Description of use	Purpose of use
Customer personal details that are provided when registering, including user names and passwords	Information will be used for security purposes to verify identity of users Information will be transferred between TRAILS and the Digital Licence App	To create and provide ongoing online access to the Digital Licence App To ensure user records are kept up to date
Customer personal details that are sourced from TRAILS or collected through the Digital Licence App	Information will be provided to ICT service providers, including web and mobile application vendors and providers of cloud computing and software services	To allow the provision of ICT services for the purpose of creating and operating the Digital Licence App
Customer personal details that are logged when using the mobile app	Access information will be logged by ICT service providers and accessed by TMR as required	To analyse usage of the Digital Licence App and to develop enhancements. To identify potential misuse and implement security safeguards. To display a data access log to the Customer.

5.4.4 Disclosure of personal information

Only limited new disclosures of personal information by TMR to third parties will occur in connection with the Digital Licence App. This table identifies the disclosures of personal information to third parties that will occur in connection with the Digital Licence App.

Disclosure made to	Information disclosed	Purpose of Disclosure
Verifiers who scan a Customer's Digital Licence	That information selected by Customer for release, which may include photograph, name, date of birth, address, class and type of vehicle and licence conditions	To fulfil request by Customer for TMR to verify their identity or other information to Verifier

TMR may disclose to a Verifier that a Digital Licence is genuine. For example, by the use of the Reader App or the Digital Licence App by a Verifier to scan a QR code or similar. As a result of the Verifier scanning the Customer's mobile device, personal

information of the Customer will be transferred by TMR to the Verifier through the Digital Licence App and Reader App.

These types of disclosures will only occur with the express authorisation and knowledge of the Customer, because the Customer will provide their mobile device to the Verifier for scanning.

Where a Customer shows a third party their Digital Licence, the third party will access personal information of the Customer by viewing the device. Customers may also create a PDF of their Digital Licence to send by SMS or email to a selected recipient. The Customer may also allow the third party to take a copy or photograph of the personal information displayed on the mobile device through the Digital Licence App. All of these disclosures will be made by the Customer and not by TMR.

TMR will continue to disclose personal information about Customers, including traffic history, to police to assist them in carrying out their enforcement functions or other agencies as permitted under specific legislative authorities. However, those disclosures do not occur through, or because of, the Digital Licence App. The ordinary processes adopted by TMR for release of that information will apply, including that a lawful basis for release of the information must exist. These disclosures are outside the scope of this PIA as they form part of exiting TMR processes.

6. Privacy impact analysis

This section sets out an analysis of how the Digital Licence App and Reader App impact on privacy, including analysis of compliance with the IP Act and other legislative provisions.

TMR does not collect, store, use or disclose personal information of Verifiers in connection with their use of the Reader App. However, the Reader App is relevant to the disclosure of personal information of Customers that occurs when they present their mobile device for verification by a Verifier.

6.1 Collection of personal information

Most of the personal information that will be displayed in the Digital Licence App is collected independently as part of the application for a Driver Licence, Marine Licence or Photo Identification Card. That information is stored in TRAILS. The Digital Licence App will involve only limited collection of additional personal information about users as set out in section 5.4.1.

The privacy requirements most relevant to collection are IPPs 1, 2 and 3.

6.1.1 IPP 1

IPP 1 requires TMR to only collect personal information that is necessary to fulfil a lawful purpose directly related to its functions and activities. The IP Guidelines state that collection will only be necessary if it helps to achieve the relevant purpose.[6]

TMR's general functions and activities include administration of laws relating to Driver Licences, Marine Licences and Photo Identification Cards. These laws will be amended to allow for the Digital Licence App and digital credentials.

Therefore, the information collected by TMR in connection with the Digital Licence App will be for a purpose associated with its functions and activities under the relevant Act relating to the credential.

TMR will not request unnecessary or excessive information that is not relevant to its purposes. The information required is directly related to its functions and activities of administering Driver Licences, Marine Licences and Photo Identification Cards.

The position will be less clear where the scope of the Digital Licence App is extended to other credentials not administered by TMR. Further analysis will need to be undertaken to assess whether collection of the personal information by TMR is related to its purposes in that scenario.

[6] http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/collection/lawful-and-fair-collection.

IPP 1 also prohibits collection of personal information by unlawful or unfair means. Information collection is unlawful if it is collected in illegal ways, for example, if it is collected through interfering with mail or using listening devices. The IP Guidelines also give examples of unfair collections, such as tricking people into giving information by not indicating on forms which questions are voluntary.

The collection of personal information by TMR in connection with the Digital Licence App would not be unlawful and there is nothing to indicate that the means of collection would be unfair. Customers voluntarily request access to a Digital Licence App and are not required to use one.

Depending on the functionality of the Digital Licence App, information may be collected by accessing other parts of a user's mobile device. A mobile app would ordinarily require a number of permissions to enable it to work appropriately, which authorise the mobile app to access different parts of the mobile device, including:

- location services; and
- Wifi connection accessibility.

However, although the mobile app may have permission to access the mobile device, information may not be automatically 'collected' in the course of that access. For example, although the app has permission to access the photos/media/files on the device, information will not be collected until such time as the user chooses to upload documents or photos. Similarly, the Wifi connection is accessed to secure an internet connection but personal information is not collected.

The way in which these permissions will operate must be clearly explained in the Digital Licence App privacy statement so that users are aware of how the app accesses personal information stored in their mobile device. If the privacy statement complies with these requirements it is fair and reasonable for the app to access this information.

The Digital Licence App will collect location and usage information as explained in the table in section 5.4.1. It will also require Bluetooth connectivity as explained at section 6.8 of this PIA. This functionality will occur with the knowledge and consent of the Customer, who will be requested to ensure location services, wifi and Bluetooth are switched on for the purposes of the Digital Licence App.

General recommendations about development of the mobile app are made at section 6.8 of this PIA.

6.1.2 IPP 2

IPP 2 applies when a government agency asks for personal information directly from the person about whom the information refers. It requires the agency to take whatever steps are reasonable to make sure the person is aware:

- why the agency is collecting the information;
- whether the collection is authorised or required by law; and

- to whom the agency usually gives that kind of information.

A privacy notice should be displayed to Customers at the start of the registration process for the Digital Licence App, because the registration process and subsequent use of the Digital Licence App will involve the collection of personal information. The privacy notice should also be displayed when Customers download the Digital Licence App.

The privacy notice will need to include all information required by IPP 2 and should be specific to the Digital Licence App. The Digital Licence App website and app should not direct Customers to the generic TMR privacy statement. The Digital Licence App privacy notice should be the only source of privacy information made available to Customers (other than to the extent privacy is dealt with in the terms and conditions of use).

Recommendation 1 - Privacy notice

A privacy notice should be incorporated into the registration process for the Digital Licence and when Customers downloads the Digital Licence App. It should also be imbedded into the Digital Licence App and website.

The privacy notice should be specific to the Digital Licence App.

The notice should make Customers aware of the following matters before any personal information is provided:

- The information is being collected by TMR.
- TMR's contact details.
- Their use of the Digital Licence App may involve the collection of their personal information.
- The information is being collected for the purpose of:
    - administration of the Digital Licence App, including verification of users and security;
    - allowing access to the Digital Licence App;
    - other purposes under the PIC Act, TORUM and other transport legislation.
- If their personal information is not provided, then their identity may not be verified and they will not be able to access the Digital Licence App and TMR's records about them may not be kept up to date or will have to be kept up to date in another way.
- To whom TMR usually provides the information, including:

- suppliers of ICT services;
- police for the purpose of law enforcement functions if specific legislative authority exists; and
- third parties to whom the Customer produces the Digital Licence for scanning.

- That TMR is likely to disclose personal information to overseas recipients in the following circumstances:
  - where a Customer accesses the Digital Licence App whilst overseas; and
  - where a service provider who provides support services for the Digital Licence App has servers located overseas.
- That TMR will not disclose personal information to other third parties except in accordance with the *Information Privacy Act 2009*.
- The permissions that the mobile app requires to access information on the Customer's mobile device and an explanation of why those permissions are required.
- A statement to the effect that, by presenting a Digital Licence to a third party for scanning, the Customer consents to their personal information being disclosed to the third party.
- Provide a link to TMR's privacy policy.

Customer's should be required to check a tick box confirming they have read and understood the privacy notice and privacy policy.

6.1.3 IPP 3

IPP 3 requires that TMR, when asking for personal information:

- take reasonable steps to ensure that the information collected is relevant, up to date and complete; and
- take reasonable steps to ensure that they do not collect information in an unreasonably and intrusive way.

When TMR collect personal information, it sometimes has to intrude into peoples' personal affairs, but IPP 3 requires TMR to do its best to make sure this intrusion is reasonable, in relation to the way the information is collected. The way in which personal information is proposed to be collected from users through the Digital Licence App does not intrude to an unreasonable extent on their personal affairs.

Although the mobile app accesses information on the Customer's phone, express notice of this functionality will be provided to Customers in the privacy notice. Logging of access information and the limited permissions adopted in the mobile app are standard and cannot be said to be unreasonable or intrusive.

A general obligation is also placed on TMR to ensure that personal information is complete and up to date. TMR should take reasonable steps to ensure that information that is related to the Digital Licence App is up-to-date.

Recommendation 2 - Notice of requirement to notify of changes in personal information

The Digital Licence App should contain a notice to Customer's asking that they notify TMR of any changes in their personal information details so that records are complete and up-to-date.

Recommendation 3 – Implementation of protocols to update personal information when required

A protocol should be introduced into the Digital Licence App database that prompts users to verify that the personal information displayed in the Digital Licence App is up to date. For example, a push notification issued to remind Customers to update their information.

6.1.4 Transport legislation

Section 46 of the PIC Act, s 143 of TORUM and s 205AC of the Marine Safety Act prohibit the storage of personal information by TMR, except where it is in the discharge or performance of functions under the Act or is authorised under another Act. For the reasons outlined above, this exception will apply and the sections do not prevent TMR from collecting personal information of Customers for the purpose of the Digital Licence App.

6.2 Use of personal information

The transfer of personal information from TRAILS to the Digital Licence App and verification of Customer's identity are uses of personal information.

The provision of personal information to ICT service providers is also a use, not a disclosure, because TMR will retain control over who will know the personal information in the future (refer to section 5.4.2).

The privacy requirements relevant to use of personal information are contained in IPPs 8, 9 and 10.

6.2.1 Transport legislation

Section 46 of the PIC Act, s 143 of TORUM and s 205AC of the Marine Safety Act prohibit the use of personal information by TMR, except where it is in the discharge or performance of functions under the Acts, authorised under another Act or with the consent of the Customer.

The table in section 5.4.3 identifies the purposes of the relevant uses of personal information that will occur as part of the Digital Licence App. All of those purposes are incidental to, and in the furtherance of, TMR's functions under the PIC Act, TORUM and the Marine Safety Act and relate to administration of the digital credentials stored in the Digital Licence App.

Further, if a privacy notice in line with Recommendation 1 is provided to Customers, then TMR will be able to show that they were aware of, and consented to, the proposed uses of their personal information.

Accordingly, the uses will be permitted under section 46 of APCA, section 205AC of the Marine Safety Act and section 143 of TORUM.

6.2.2 IPP 8

Before TMR may use personal information, it must first take reasonable steps to make sure that the information is accurate, up to date and complete. Compliance with this requirement is not materially affected by the Digital Licence App, but TMR should ensure that the Customer's personal information remains as up-to-date as possible (refer to recommendations 2 and 3).

6.2.3 IPP 9

IPP 9 requires TMR to identify:

- the purpose for which the personal information is being used; and
- the relevance of the personal information to that purpose.

The process of undertaking this PIA is relevant to TMR's compliance with IPP 9. There are no proposals for use of personal information for purposes to which that personal information is not relevant.

6.2.4 IPP 10

The first paragraph in IPP 10.1 states a general rule that an agency may only use personal information for the particular purpose for which it obtained the information. Paragraphs (a) to (f) are five exceptions where an agency may use personal information for purposes other than that for which it obtained that information.

The circumstances in which IPP 10 would potentially apply are limited because under the confidentiality provisions in section 46 of the PIC Act, section 143 of TORUM and section 205AC of the Marine Safety Act, a person may not use information gained through their involvement in the administration of those Acts except for a purpose under them or if authorised under another Act. In most cases, use of personal information in the discharge of functions under the PIC Act or TORUM would be use of the information for the particular purpose for which the information was obtained.

It is necessary to identify the purposes for which information that is used in the Digital Licence App was collected. This includes information collected not only through the Digital Licence App, but other personal information collected independently.

The relevant purposes are identified in the table at section 5.4.3. All of those purposes are incidental to, and in the furtherance of, TMR's functions under the PIC Act, TORUM and the Marine Safety Act and relate to administration of the digital credentials stored in the Digital Licence App.

The exception in IPP10(e) will apply to all proposed uses of the personal information in connection with the Digital Licence App as they are directly related to those functions and activities. In particular:

- The transfer of information from TRAILS to the Digital Licence App involves the transfer of information to a new system that allows online, rather than manual, access.
- The provision of information to ICT service providers will also fall within IPP10(e) because it is for the purpose of providing the ICT services that will allow users to access licence information in a more easily accessible way.
- The verification of Customer's identity is also a use of information that is directly related to the purpose of administering the Digital Licence App.
- The use of access information to maintain security and optimise the Digital Licence App is directly related to operating the system.

Therefore, none of the proposed uses of personal information will breach IPP 10.

Further, as outlined in section 5.2.1, privacy notices provided to Customer's can be relied upon to show that they were aware of, and consented to, the proposed uses of their personal information.

6.3 Disclosure of personal information

There are limited new disclosures of information that will occur in connection in the Digital Licence App on the basis of the proposed pilot. The new disclosure that will occur in connection with the Digital Licence App are those made by TMR to Verifiers who scan a Customer's Digital Licence.

The privacy requirements most relevant to disclosure are the privacy requirements in IPP 11, section 46 of PIC Act, section 143 of TORUM and section 205AC of the Marine Safety Act.

TMR will disclose to a Verifier that a credential within a Digital Licence App is genuine. For example, by the use of the Reader App or the Digital Licence App by the Verifier to scan a QR code or similar. As a result of the Verifier scanning the Customer's mobile device, personal information of the Customer will be transferred by TMR to the Verifier through the Digital Licence App and Reader App.

However, these types of disclosures will only occur with the knowledge of the Customer, which is evidenced by them providing their mobile device to the Verifier for scanning. The Customer selects the personal information that they agree to share with the Verifier. The Customer must consent to the disclosure of that information before a QR code is generated for the Verifier to scan. The privacy notice for the Digital Licence App also draws attention to the disclosures that will be made to Verifiers.

By authorising a Verifier to scan their Digital Licence, Customers consent to disclosure of information to the Verifier. Specific notices are provided to Customers through the Digital Licence App to make sure they are aware of the consequences of supplying their mobile device for verification by a Verifier.

The privacy notice for the Digital Licence App will also include specific consents from Customers about disclosures to Verifiers.

Therefore, such disclosures are permitted under IPP 11, the PIC Act, TORUM and the Marine Safety Act.

Recommendation 4 – Privacy consents

The privacy notice incorporated into the registration process for the Digital Licence App should contain a statement to the effect that by presenting a Digital Licence to a third party for scanning, the Customer consents to their personal information being disclosed to the third party.

TMR will also continue to disclose personal information about Customers, including traffic history, to police to assist them in carrying out their enforcement functions. However, that disclosure does not occur through, or because of, the Digital Licence App. The ordinary processes adopted by TMR for release of that information will apply, including that the police must demonstrate a lawful basis for release of the information.

If police want access to particular information about a Customer that is collected through the Digital Licence App (such as access logs), then it will be necessary for the police to demonstrate to TMR that legal authority exists for disclosure of that information without the consent of the Customer. TMR will not be permitted to disclosure access log or other information to the police unless that disclosure is required or permitted by law.

6.4 Security of personal information

The relevant privacy requirement regarding security is IPP 4.

IPP 4(1)(a) requires agencies that have possession or control of records that contain personal information to ensure that the records are protected against loss, unauthorised access, use, modification or disclosure and misuse by such security safe guards as are reasonable in the circumstances to take.

The Digital Licence App will be developed by a vendor contracted to TMR and will involve the use of cloud based infrastructure. The information accessed through the Digital Licence App will not be stored in the cloud, but it will transfer through this infrastructure. Information will only be cached locally on a Customer's mobile device so that when the Digital Licence App is opened, the last cached information will be displayed.

The IP Guidelines indicate that key security mechanisms for TMR to adopt are:

- Limiting access to personal information to only those persons who require access. Steps should be taken to ensure digital information is not readily accessible to everyone within TMR.
- Audit logs may be used to determine if security has been breached and personal information accessed, used or disclosed contrary to the IP Act. Audit logs should be audited to detect misuse.

TMR has an Information Security Policy and Information Security Plan developed under *Information Security Policy IS18:2018* published by the Queensland Government Chief Information Officer. Those documents establish the basic security measures that are adopted TMR. However, extra security measures are appropriate for the information in the Digital Licence App.

The level of security that is required depends upon the nature of the personal information in the record and the risk of a security breach occurring. TMR has classified the information as PROTECTED. That classification will indicate the controls that are relevant for the information.

The information in the Digital Licence App will be sensitive and will include information subject to the statutory obligations of confidentiality in the PIC Act, TORUM and the Marine Safety Act.

There are no decisions of the Queensland Office of the Information Commissioner to show how the Commissioner will view the obligation of agencies to implement IPP 4 when a vendor is supplying the solution.

There are some decisions of the Federal Commissioner that are of interest as the former NPP4 was in similar terms to IPP 4. The decisions show that TMR needs to be able to show that it has taken reasonable steps to ensure that data that is dealt with by contractors is secure by doing such things as ensuring that the contractor:

- maintains the software being used to protect the data and updates it to the latest and most secure version from time to time;
- has a comprehensive security policy that is reviewed regularly and is promulgated to it staff;
- has a data access system that allows identification of users who access the data so as to provide an effective audit trail;
- has an audit program that can identify breaches and weaknesses in systems;
- is required to report data breaches in a timely way so that TMR can take action to notify the affected individual and remedy the vulnerability, audit the systems and put in place adequate protections, if necessary
- cleanses the cache as required; and
- encrypts sensitive data whenever it is being transferred.

Including appropriate clauses in the contractual arrangements with the vendors will be critical to enabling TMR to discharge its obligations under IPP 4. However, since the specific details of the contract of engagement are confidential, it is not appropriate to set them out in this PIA.

TMR has taken steps to ensure that security safeguards are built into the design of the Digital Licence App, including:

- The Digital Licence App will be designed and developed in accordance with ISO 18013-5 and Trusted Digital Identity Framework (TDIF) version 1.5. ISO 18013-5 is currently being developed by a working group and is in draft form. However, once finalised, it will set out the interface and related requirements to facilitate ISO/IEC compliant driving licence functionality on a mobile device.
- Personal information of Customer's will be cached locally in their mobile device. Personal information will be encrypted before it is transferred from TRAILS to the Customer's mobile device. The ICT contractor will neither store nor access unencrypted personal information. The ICT contractor will store the Customer's CRN, but not in connection with any other unencrypted personal information of the Customer.
- Customers will be required to enter a 6-digit PIN before accessing the Digital Licence App on their mobile device. The app will automatically require the PIN to be re-entered if it goes into sleep mode or the Customer exits from the app.
- Prompts and warnings will be built into the Digital Licence App to ensure that Customers are aware, and authorise, particular disclosures of their personal information. For example, the Customer will be prompted before providing their mobile device to a third party for validation of their digital credential.
- Customers will be prompted to agree to any additional access that the Digital Licence App has to their mobile device. For example, Customers will be prompted

to turn Location Services on and will be required to insert their 6-digit pin before downloading information into a PDF format.

- TMR will have the ability, at the request of Customers, to 'wipe' their Digital Licence App account in the event that their mobile device is lost or stolen. The Customer will be able to contact TMR and, upon establishing their identity, request that access to credentials within the Digital Licence App be withdrawn.

Recommendation 5 – Security safeguards

TMR should ensure that security safeguards are built into the design and development of the Digital Licence App and that the arrangements with contractors specify that the security safeguards are contractual obligations.

6.5 Engagement of service providers

6.5.1 IPP (4)(1)(b) and s 35 of the IP Act

IPP 4(1)(b) requires TMR to do everything in its power to prevent unauthorised use or disclosure of personal information that it gives to contractors.

The IP Act also goes one step further and states under what circumstances service providers are also to be bound by the IPPs. Section 35 of the IP Act requires TMR to ensure that a service provider is required to comply with the IPPs as if it were TMR if the contractor will in any way deal with personal information on behalf of TMR or the provision of services under the arrangement will involve the transfer of personal information to TMR.

If TMR does not taken reasonable steps to bind a service provider, then TMR will be liable for any breach of the IP Act or IPPs by the service provider.[7] It is also important, as explained as section 5.4.2, that TMR retain control over personal information to ensure the provision of information to service providers is as use, not a disclosure.

Recommendation 6 – Service contracts

Contracts with service providers should provide for the following:

- appropriate restrictions on the service provider's use and disclosure of personal information to ensure TMR retains control over that information;
- a requirement for the service provider to comply with the IP Act and the IPPs

[7] Section 37(2) of the IP Act.

as if it were TMR;

- the consequences of being a bound contracted service provider (eg that the IP Act may be enforced directly against the contracted service provider); and
- the particular circumstances arising under the contract.

6.6 Transfer of personal information outside of Australia

6.6.1 Section 33 of the IP Act

Section 33 of the IP Act sets out the circumstances in which TMR may transfer a person's personal information outside of Australia.

The IP Guidelines give examples of when information will be transferred out of Australia, including when a database is stored on a server in another country or personal information is accessed from a computer located overseas. However, the Queensland Information Commissioner's view is that information will not be transferred overseas if it is routed through another country and immediately directed back to Australia.

An ICT contractor has been engaged to develop the Digital Licence App. The contract of engagement prohibits the transfer of personal information by the contractor outside of Australia. In any event, personal information about a digital credential is only stored in the Customer's mobile device and unencrypted personal information is not provided or accessed by the contractor.

6.7 Access to personal information

The relevant privacy requirements regarding access to personal information are IPPs 5, 6 and 7 and sections 40 and 41 of the IP Act.

Under IPP 5, TMR is required to take reasonable steps to enable a Customer to ascertain whether it holds records containing their personal information. Under IPP 6 and 7, a person's right of access to information kept by a Government agency about them and their right of amendment or correction in respect of that information is limited to the rights under sections 40 and 41 of the IP Act.

The operation of the Digital Licence App is not materially affected by the requirements regarding access to, or correction of, personal information. However, TMR will need to ensure that information stored in the cloud is not overlooked when searches are being undertaken to locate information relevant to an access or amendment application.[8]

[8] http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/cloud-computing-and-the-privacy-principles.

6.8 Mobile phone applications

The IP Guidelines specifically deal with privacy issues concerning mobile phone apps.[9]

The Digital Licence App has been developed in light of the recommendations made in the IP Guidelines. Specific consideration has been given to whether and for what purpose the app:

- requests permission from the Customer to access information stored on their device; and
- logs usage information, such as:
  - name of the device
  - platform used to access the Digital Licence App
  - device's unique identifier
  - location

Information is only accessed and logged for legitimate purposes. For example, to:

- monitor and analyse usage of the Digital Licence App and develop enhancements; and
- detect unauthorised account activity and apply security safeguards (i.e. requirement to use verification code if user accesses app from an unusual location).

The Digital Licence App will require users to turn Bluetooth on within their mobile device. This is necessary because the app requires low powered Bluetooth connectivity to facilitate the verification of digital credentials.

Customers will also be prompted to turn Location Services on when using the Digital Licence App and, if they choose not to do so, only limited functionality within the app will be available.

The use of a prompt to turn on Location Services will ensure that Customers are aware that the app will be accessing the location information within their mobile device. Customers will have the option not to allow the Digital Licence App such access and to instead use their physical credential.

The Digital Licence App does not otherwise collect or store information about the Customer's location.

The access log for the Digital Licence App is stored locally on the Customer's mobile device and keep a log of any third party validations that occur through that device only. The access log is not stored by TMR or its ICT contractor.

[9] http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-mobile-apps.

The Digital Licence App may also access other parts of a Customer's mobile device, but only at their request. The Customer will be able to create a PDF document of a digital credential and send that document to a third party by text or email. The Customer is required to enter their 6-digit PIN before to download information into a PDF format.

Recommendation 7 – Development of mobile app

The Digital Licence App should be designed to limit access to information stored on the mobile device to legitimate purposes.

6.9 Future functionality of the Digital Licence App

The Digital Licence App and Reader App are in the early stages of development. Future functionality built into the Digital Licence App or Reader App may result in additional personal information being collected, used or disclosed by TMR.

This PIA will need to be updated at each point when:

- further detail about the technology and processes used to operate the Digital Licence App or Reader App are identified or change; and
- functionality is added to the Digital Licence App or Reader App.

Additional functionality includes:

- addition of credentials to the Digital Licence App;
- expansion of tasks or activities to be performed in the Digital Licence App or Reader App;
- changes to the way personal information is collected, stored, used or disclosed in conjunction with the Digital Licence App or Reader App; and
- collaboration with other government agencies.

Recommendation 8 – Review of privacy issues during expansion of functionality

A protocol should be put in place during the development of future functionality in the Digital Licence App and Reader App that requires privacy issues to be considered in relation to the proposed additional functionality. Further PIAs should be prepared in relation to additional functionality of the Digital Licence App or Reader App.

7. Human Rights

7.1.1 Application of the *Human Rights Act 2019*

The *Human Rights Act 2019* (Qld) commenced on 1 January 2020 and provides legislative protection of 23 human rights in Queensland. BCS is a public entity for the purpose of the *Human Rights Act*.

The *Human Rights Act* will be relevant to the Digital Licence App in two ways – firstly, how the legislative provisions authorising use of the systems are interpreted and, secondly, the considerations that apply when TMR makes a decisions or takes action in relation to operation of the App.

7.1.2 Scope of the right to privacy

Section 25 of the *Human Rights Act* contains a right to privacy and reputation, which is described as follows:

> **25 Privacy and reputation**
>
> A person has the right—
>
> (a) not to have the person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
>
> (b) not to have the person's reputation unlawfully attacked.

This human right contains internal limitations and permits lawful and non-arbitrary interferences with a person's privacy.

7.1.3 Statutory interpretation

Section 48 of the *Human Rights Act* requires legislation to be interpreted in a way that is compatible with human rights, to the extent possible that is consistent with its purpose. If a provision cannot be interpreted in a way that is compatible with human rights, the provision must be interpreted in a way that is most compatible with human rights, to the extent possible that is consistent with its purpose.

In practice, if there is only one possible interpretation of a legislative provision, then that interpretation will apply irrespective of whether it is compatible with human rights or not. Where multiple interpretations of a provision are possible, than the one that is consistent with its purpose but is most compatible with human rights must be adopted.

In the case of the provisions in the relevant transport legislation that authorise particular uses or disclosures of information, we consider that the provisions are clear and there is only one interpretation that can be given to them.

Accordingly, the *Human Rights Act* does not affect our interpretation of these provisions.

7.1.4 Acts or decisions

Section 58 of the *Human Rights Act* states that it is unlawful for a public entity:

a) to act or make a decision in a way that is not compatible with human rights; or

b) to fail to give proper consideration to a human right relevant to the decision.

Paragraph (a) is the 'substantive' limb and paragraph (b) is the 'procedural' limb.

The substantive limb directs an agency to justify any limit on a human right in accordance with ss 8 and 13 of the *Human Rights Act*, which essentially require that any limit on a human right has a proper purpose and is necessary and appropriate. Section 8 states that an act or decision is compatible with human rights if it either does not limit a human right or limits a human right only to the extent that is reasonable and demonstrably justifiable in accordance with s 13.

For the procedural limb, s 58(5) provides that giving proper consideration requires identifying the human rights that may be affected and considering whether the limit on those human rights is justified.

Section 13 sets out the test for determining whether a limit on a human right is justified. It provides:

> (1) A human right may be subject under law only to reasonable limits that can be demonstrably justified in a free and democratic society based on human dignity, equality and freedom.
>
> (2) In deciding whether a limit on a human right is reasonable and justifiable as mentioned in subsection (1), the following factors may be relevant—
>
> (a) the nature of the human right;
>
> (b) the nature of the purpose of the limitation, including whether it is consistent with a free and democratic society based on human dignity, equality and freedom;
>
> (c) the relationship between the limitation and its purpose, including whether the limitation helps to achieve the purpose;
>
> (d) whether there are any less restrictive and reasonably available ways to achieve the purpose;
>
> (e) the importance of the purpose of the limitation;
>
> (f) the importance of preserving the human right, taking into account the nature and extent of the limitation on the human right;
>
> (g) the balance between the matters mentioned in paragraphs (e) and (f).

If an act or decision does *not* have any impact on a human right, the act or decision will be compatible with human rights. However, if an act or decision *does* have an impact on a human right, that limit will need to be justified under s 13.

For the reasons outlined in this PIA, we consider the interferences to privacy arising from the Digital Licence App to be lawful. However, it remains necessary to consider whether those interferences are arbitrary.

Although it is not entirely settled, case law in other jurisdictions indicates that 'arbitrary' interferences are those that are capricious, unpredictable, unjust or are unreasonable in the sense that they are not proportionate to a legitimate aim: *PJB v Melbourne Health (Patrick's Case)* [2011] VSC 327 at [85] and *WBM v Chief Commissioner of Police* (2012) 43 VR 446.

Accordingly, deciding whether an interference with privacy is arbitrary will involve similar considerations to whether a limit on a human right is justified under s 13 of the *Human Rights Act*. There is also authority that internal limitations like 'arbitrary' are considered under s 13, not merely that the factors in s 13 are relevant: *Re Kracke and Mental Health Review Board* (2009) 29 VAR 1, 35 [109]-[110] (Bell J).

The Digital Licence App involves interferences with the privacy of registered users. However, it is unlikely that such interferences will be found to be arbitrary for the reasons set out below.

A user will voluntary apply for a Digital Licence App and will be given privacy notices explaining how their personal information will be handled. Accordingly, their decision to use the Digital Licence App will be made voluntarily and on the basis of informed consent. An individual has a choice as to whether to apply for a Digital Licence App.

Further, credentials stored in a Digital Licence App are only disclosed at the instigation of the registered user themselves. The Digital Licence App has significant security features to protect the credentials stored in it.

The Digital Licence App interferes with privacy only to the extent necessary to ensure its proper administration and after users have been provided a privacy notice about the use of their personal information. This is consistent with a free and democratic society based on human dignity, equality and freedom.

Accordingly, any limits on an individual's right to privacy arising as a result of the Digital Licence App are unlikely to be arbitrary interferences within the meaning of s 25 of the *Human Rights Act* or will otherwise be reasonable and justified under s 13 of the *Human Rights Act*.

8. Recommendations

The recommendations made throughout the report are as follows:

Recommendation	
Recommendation 1 - Privacy notice	A privacy notice should be incorporated into the registration process for the Digital Licence and when Customers download the Digital Licence App. It should also be imbedded into the Digital Licence App and website. The privacy notice should be specific to the Digital Licence App. The notice should make Customers aware of the following matters before any personal information is provided: ▪ The information is being collected by TMR. ▪ TMR's contact details. ▪ Their use of the Digital Licence App may involve the collection of their personal information. ▪ The information is being collected for the purpose of: o administration of the Digital Licence App, including verification of users and security; o allowing access to the Digital Licence App; o other purposes under the PIC Act, TORUM and other transport legislation. ▪ If their personal information is not provided, then their identity may not be verified and they will not be able to access the Digital Licence App and TMR's records about them may not be kept up to date or will have to be kept up to date in another way. ▪ To whom TMR usually provides the information, including: o suppliers of ICT services; o police for the purpose of law enforcement functions if specific legislative authority exists; and o third parties to whom the Customer produces the

	Digital Licence for scanning. ▪ That TMR is likely to disclose personal information to overseas recipients in the following circumstances: o where a Customer accesses the Digital Licence App whilst overseas; o where a service provider who provides support services for the Digital Licence App has servers located overseas. ▪ That TMR will not disclose personal information to other third parties except in accordance with the *Information Privacy Act 2009*. ▪ The permissions that the mobile app requires to access information on the Customer's mobile device and an explanation of why those permissions are required. ▪ A statement to the effect that, by presenting a Digital Licence to a third party for scanning, the Customer consents to their personal information being disclosed to the third party. ▪ Provide a link to TMR's privacy policy. Customer's should be required to check a tick box confirming they have read and understood the privacy notice and privacy policy.
Recommendation 2 - Notice of requirement to notify of changes in personal information	The Digital Licence App should contain a notice to Customer's asking that they notify TMR of any changes in their personal information details so that records are complete and up-to-date.
Recommendation 3 – Implementation of protocols to update personal information when required	A protocol should be introduced into the Digital Licence App database that prompts users to verify that the personal information displayed in the Digital Licence App is up to date. For example, a push notification issued to remind Customers to update their information.
Recommendation 4 – Privacy consents	The privacy notice incorporated into the registration process for the Digital Licence App should contain a statement to the effect that by presenting a Digital Licence to a third party for scanning, the Customer consents to their personal information being disclosed to the third party.
Recommendation 5 – Security	TMR should ensure that security safeguards are built into the

safeguards	design and development of the Digital Licence App and that the arrangements with contractors specify that the security safeguards are contractual obligations.
Recommendation 6 – Service contracts	Contracts with service providers should provide for the following: ▪ appropriate restrictions on the service provider's use and disclosure of personal information to ensure TMR retains control over that information; ▪ a requirement for the service provider to comply with the IP Act and the IPPs as if it were TMR; ▪ the consequences of being a bound contracted service provider (eg that the IP Act may be enforced directly against the contracted service provider); and ▪ the particular circumstances arising under the contract.
Recommendation 7 – Development of mobile app	The Digital Licence App should be designed to limit access to information stored on the mobile device to legitimate purposes.
Recommendation 8 – Review of privacy issues during expansion of functionality	A protocol should be put in place during the development of future functionality in the Digital Licence App and Reader App that requires privacy issues to be considered in relation to the proposed additional functionality. Further PIAs should be prepared in relation to additional functionality of the Digital Licence App or Reader App.