

From: [Kevin Linnane](#)
To: [Jonas Holland](#)
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes
Attachments: [image001.png](#)
[Sharing the IVS photo.msg](#)

Kia ora

I was sent the attached a couple of weeks back. Should hopefully shed a bit more light on the thinking at their end. I've had a couple of chats to Will since. Broadly they are playing this by the book.

Ngā mihi
Kevin

From: Jonas Holland
Sent: Wednesday, 7 February 2018 13:23
To: William Hopgood
Cc: Grant Stark; Kevin Linnane
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hi William

Sorry I missed this question in your earlier email.

It would be good to get more information about this. I don't know anything about the integration consent between RealMe and IVS, how it defines "biodata" or the applicable purposes of use. Also – what will sharing the photo of the account page involve. Happy to talk this through.

Kevin – not sure if you know anything about this.

Jonas

From: William Hopgood
Sent: Thursday, 1 February 2018 5:13 PM
To: Jonas Holland
Cc: Grant Stark
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Thanks again Jonas,

One small thing, have you had a chance to think about Grants question below:

Also, on a side note, Grant and I are working through some of the changes required to enable sharing of the IVS Photo via RealMe. We would like a Legal opinion on whether changes would be need to the integration consent between RealMe and IVS. Currently, the integration consent allows for the sharing of Biodata from IVS to RealMe, however, it only stipulates that this is for the purpose of showing the photo on the RealMe account page.

Feel free to get in touch with either myself or Grant for more information

Cheers

William Hopgood | Senior Advisor Business and Product Development

From: Jonas Holland
Sent: Tuesday, 30 January 2018 11:36 a.m.
To: William Hopgood
Cc: Nicola Potter; Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hi

I have included my changes and comments in the documents.

The main change was to more clearly set out the concept of an attribute provider (of which NZ Post is just one example). It may be that we may need to be even clearer on this point – particularly in the RealMe Terms and Privacy Statement.

Happy to meet to discuss if that is the easiest next step.

Regards

Jonas

From: William Hopgood
Sent: Wednesday, 24 January 2018 8:53 AM
To: Nicola Potter; Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello,

The deadline for these reviews has been extended out to 1st Feb 5pm to allow for a Legal review

RealMe Privacy statement

9(2)(k)

Identity Verification Service Privacy Statement

9(2)(k)

IVS Terms of Use

9(2)(k)

RealMe Terms of Use

9(2)(k)

Thank you

William Hopgood | Senior Advisor Business and Product Development

From: William Hopgood
Sent: Friday, 19 January 2018 7:34 a.m.
To: Nicola Potter; Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello,

One more thing, it was identified that changes were also needed to the RealMe Privacy statement. I have pushed the due date for review out to 5pm Thursday 26th Jan.

RealMe Privacy statement

9(2)(k)

Thank you

William Hopgood | Senior Advisor Business and Product Development

From: William Hopgood
Sent: Thursday, 18 January 2018 4:19 p.m.
To: Nicola Potter
Cc: Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello all,

I have added the documents to cohesion along with Nicolas comments. Please add you changes to them there by the 5pm Wednesday 25th Jan

Identity Verification Service Privacy Statement

9(2)(k)

IVS Terms of Use

9(2)(k)

Thank you

William Hopgood | Senior Advisor Business and Product Development

From: Nicola Potter
Sent: Thursday, 18 January 2018 11:57 a.m.
To: William Hopgood
Cc: Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Thanks Will. I have reviewed and attached my feedback.

Happy to discuss further.

Cheers

Nicola Potter | Manager IVS Operations
Identity & Passport Services | Te Mata Uruwhenua
The Department of Internal Affairs | Te Tari Taiwhenua
Direct Dial: +64 4 382 3443 | Extn: 4443 | www.dia.govt.nz

Logo-test



From: William Hopgood
Sent: Wednesday, 17 January 2018 8:59 a.m.
To: Grant Stark; Helen Coffey; Tim Waldron; Nicola Potter; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial
Subject: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello,

Please find attached updates to the RealMe and IVS Terms of Use and the IVS Privacy Statement for feedback.

The RealMe ToU:

This has had changes to remove mention of the NZ Post Partnership and removal of reference to igovt verified identity. I have added one comment that Service Innovation could answer:

- The Terms of Use referred to the verified identity as a "igovt verified identity". I had removed the word "igovt" but did we want to replace it with DIA to show it as a 'DIA verified identity' considering it sits beside in contest with a "NZPost verified address"

The IVS ToU:

Changes have been made to the Terms of Use to include mention of the mobile app.

- I was unable to determine what relevant content should be added to cover use of the app. Any guidance or input here would be appreciated.

The IVS Privacy Statement:

Changes have been made to include the mention of the mobile app, facial recognition and the Pre-EIC.

- This is the final draft.

Also, on a side note, Grant and I are working through some of the changes requitred to enable sharing of the IVS Photo via RealMe. We would like a Legal opinion on whether changes would be need to the intergration consent between RealMe and IVS. Currently, the intergration consent allows for the sharing of Biodata from IVS to RealMe, however, it only stipulates that this is for the purpose of showing the photo on the RealMe accoutn page.

Since the photo will not be visable on the account page, is a change required to the intergration consent to include photo.

See attached email fro more context

Regards

William Hopgood | Senior Advisor Business and Product Development
Identity & Passport Services | Te Ratonga Tuakiri
The Department of Internal Affairs | Te Tari Taiwhenua

Direct Dial: +64 4 382 3576 | Extn: 4576
120 Victoria Street, Wellington 6011, New Zealand | www.dia.govt.nz

Logo-test



Released under the Official Information Act 1982

From: [Kevin Linnane](#)
To: [Jonas Holland](#); [William Hopgood](#)
Cc: [Nicola Potter](#); [Grant Stark](#); [Helen Coffey](#); [Tim Waldron](#); [Julie Woods](#)
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes
Attachments: [image001.png](#)

Tēnā koutou

I've added some comments and contents to the 2 privacy statements. This includes some wording around the use of customer feedback surveys. Feel free to play with the language so long as the opt-out function remains as described.

Ngā mihi
Kevin

From: Jonas Holland
Sent: Tuesday, 30 January 2018 11:36
To: William Hopgood
Cc: Nicola Potter; Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hi

I have included my changes and comments in the documents.

The main change was to more clearly set out the concept of an attribute provider (of which NZ Post is just one example). It may be that we may need to be even clearer on this point – particularly in the RealMe Terms and Privacy Statement.

Happy to meet to discuss if that is the easiest next step.

Regards

Jonas

From: William Hopgood
Sent: Wednesday, 24 January 2018 8:53 AM
To: Nicola Potter; Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello,

The deadline for these reviews has been extended out to 1st Feb 5pm to allow for a Legal review

RealMe Privacy statement

9(2)(k)

Identity Verification Service Privacy Statement

9(2)(k)

IVS Terms of Use

9(2)(k)

RealMe Terms of Use

9(2)(k)

Thank you

William Hopgood | Senior Advisor Business and Product Development

From: William Hopgood
Sent: Friday, 19 January 2018 7:34 a.m.
To: Nicola Potter; Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial
Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello,

One more thing, it was identified that changes were also needed to the RealMe Privacy statement. I have pushed the due date for review out to 5pm Thursday 26th Jan.

RealMe Privacy statement

9(2)(k)

Thank you

William Hopgood | Senior Advisor Business and Product Development

From: William Hopgood

Sent: Thursday, 18 January 2018 4:19 p.m.

To: Nicola Potter

Cc: Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial

Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello all,

I have added the documents to cohesion along with Nicolas comments. Please add you changes to them there by the 5pm Wednesday 25th Jan

Identity Verification Service Privacy Statement

9(2)(k)

IVS Terms of Use

9(2)(k)

RealMe Terms of Use

9(2)(k)

Thank you

William Hopgood | Senior Advisor Business and Product Development

From: Nicola Potter

Sent: Thursday, 18 January 2018 11:57 a.m.

To: William Hopgood

Cc: Grant Stark; Helen Coffey; Tim Waldron; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial

Subject: RE: RealMe/IVS Terms of Use + Privacy Statment Changes

Thanks Will. I have reviewed and attached my feedback.

Happy to discuss further.

Cheers

Nicola Potter | Manager IVS Operations

Identity & Passport Services | Te Mata Uruwhenua

The Department of Internal Affairs | Te Tari Taiwhenua

Direct Dial: +64 4 382 3443 | Extn: 4443 | www.dia.govt.nz

Logo-test



From: William Hopgood

Sent: Wednesday, 17 January 2018 8:59 a.m.

To: Grant Stark; Helen Coffey; Tim Waldron; Nicola Potter; Julie Woods; Kevin Linnane; Jonas Holland; Legal Services Commercial

Subject: RealMe/IVS Terms of Use + Privacy Statment Changes

Hello,

Please find attached updates to the RealMe and IVS Terms of Use and the IVS Privacy Statement for feedback.

The RealMe ToU:

This has had changes to remove mention of the NZ Post Partnership and removal of reference to igovt verified identity. I have added one comment that Service Innovation could answer:

- 9(2)(k) [Redacted]

The IVS ToU:

Changes have been made to the Terms of Use to include mention of the mobile app.

- 9(2)(k) [Redacted]

The IVS Privacy Statement:

Changes have been made to include the mention of the mobile app, facial recognition and the Pre-EIC.

- This is the final draft.

Also, on a side note, Grant and I are working through some of the changes required to enable sharing of the IVS Photo via RealMe. We would like a Legal opinion on whether changes would be need to the intergration consent between RealMe and IVS. Currently, the intergration consent allows for the sharing of Biodata from IVS to RealMe, however, it only stipulates that this is for the purpose of showing the photo on the RealMe account page.

Since the photo will not be visible on the account page, is a change required to the intergration consent to include photo.

See attached email fro more context

Regards

William Hopgood | Senior Advisor Business and Product Development
Identity & Passport Services | Te Ratonga Tuakiri
The Department of Internal Affairs | Te Tari Taiwhenua
Direct Dial: +64 4 382 3576 | Extn: 4576
120 Victoria Street, Wellington 6011, New Zealand | www.dia.govt.nz



Released under the Official Information Act 1982

From: [Kevin Linnane](#)
To: [William Hopgood](#)
Cc: [Jonas Holland](#); [Venkat Maddali](#); [Grant Stark](#)
Subject: RE: Change to the IVS Privacy Statement - RealMe Now
Attachments: [image001.png](#)
[image002.jpg](#)
[Identity Verification Service Privacy Statement - 2.1 Draft Privacy Review.docx](#)

Tēnā koutou

Apologies this has taken me so long to get to. Been a hectic few weeks getting some work for ELT moving.

IVS Statement attached with some comments. Nothing that jumps out as worrying, just some opportunities to add a little clarity.

Nō reira,
Nāku iti nei,
Nā Kevin

Kevin Linnane | Principal Advisor Privacy | Legal Services

Department of Internal Affairs Te Tari Taiwhenua

Direct Dial +64 04 494 5718 | Extension 5718 | Cell [REDACTED]
45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

cid:image002.jpg@01D3525A.A53B5660



From: William Hopgood
Sent: Friday, 16 March 2018 11:50
To: Kevin Linnane
Cc: Jonas Holland; Venkat Maddali; Grant Stark
Subject: RE: Change to the IVS Privacy Statement - RealMe Now

Hey there,

On a side note, the App uses firebase analytics to capture statistical data. It appears to be synonymized data but I thought it worth touching base to see if this is something that would also need to be included.

Below is a link showing all the user information Firebase captures by default:

<https://support.google.com/firebase/answer/6317486?hl=en>

William Hopgood | Advisor

From: William Hopgood
Sent: Friday, 16 March 2018 11:46 AM
To: Kevin Linnane
Cc: Jonas Holland
Subject: RE: Change to the IVS Privacy Statement - RealMe Now

Hey Kevin,

Any comment on this? I'm happy to organise a catch up

William Hopgood | Advisor

From: William Hopgood
Sent: Monday, 12 March 2018 8:55 AM
To: Kevin Linnane
Cc: Jonas Holland
Subject: RE: Change to the IVS Privacy Statement - RealMe Now

Hey Kevin and Jonas,

One last thing sorry, I made another change and would like your opinion on.

I added a section on the collection and use of statistical data. We are aiming to add analytics to our service during the Beta phase

Cheers

William Hopgood | Advisor

From: William Hopgood
Sent: Friday, 9 March 2018 4:08 PM
To: Kevin Linnane
Cc: Jonas Holland
Subject: Change to the IVS Privacy Statement - RealMe Now

Hey Kevin,

Attached is a draft of changes to the RealMe Now section of the Privacy Statement as per below, [REDACTED]

Happy to catch up on Monday

Cheers

William Hopgood | Advisor | Information & Partnerships
The Department of Internal Affairs | Te Tari Taiwhenua
Direct Dial: +64 4 382 3576 | Extn: 4576
120 Victoria Street, Wellington 6011, New Zealand | www.dia.govt.nz

Logo-test



Below is some context and the action points of the meeting:

next steps are:

1. 9(2)(k) [REDACTED]

2. [REDACTED]

3. [REDACTED]

9(2)(k) [REDACTED]

[REDACTED]

Released under the Official Information Act 1982

9(2)(k)

9(2)(k)

Released under the Official Information Act 1982

From: [Kevin Linnane](#)
To: [Julie Woods](#); [William Hopgood](#)
Subject: RE: IVS Web Capture
Attachments: [image001.wmz](#)
[image003.png](#)
[image004.png](#)

Kia ora

I'm happy for this to be an immediate update. This is a technology change rather than a policy change.

We aren't changing the information we collect or how it is managed. There are no additional impacts on individual's rights.

Ngā mihi
Kevin

From: Julie Woods
Sent: Wednesday, 13 March 2019 08:51
To: Kevin Linnane <Kevin.Linnane@dia.govt.nz>; William Hopgood <William.Hopgood@dia.govt.nz>
Subject: RE: IVS Web Capture

Hi guys,
So just checking I can update the Privacy Statement on the website straight away? Don't need to do the process of "we're making changes a month from now"?

Cheers
Julie

From: Kevin Linnane
Sent: Friday, 8 March 2019 1:56 PM
To: William Hopgood <William.Hopgood@dia.govt.nz>
Cc: Julie Woods <Julie.Woods@dia.govt.nz>
Subject: RE: IVS Web Capture

Brilliant. Happy with that. Technology agnostic enough for us to be able to change platforms without needing to amend statements in future.

From: William Hopgood
Sent: Friday, 8 March 2019 13:49
To: Kevin Linnane <Kevin.Linnane@dia.govt.nz>
Cc: Julie Woods <Julie.Woods@dia.govt.nz>
Subject: RE: IVS Web Capture

Hey Kevin,

As per our conversation, please find below proposed changes to the privacy statement.

RealMe digital photo capture

If you are eligible and choose to use RealMe digital photo capture services, your photo and video/frames of your liveness test will be stored within the application server to allow for automated facial recognition matching, reference by DIA for assessment of your application, quality assurance and other duties to support the Identity Verification Service.

Your captured image and liveness video may also be reused to retest biometric facial recognition thresholds to better improve our service.

Let me know your thoughts.

William Hopgood | Senior Advisor

From: Kevin Linnane
Sent: Tuesday, 5 March 2019 4:26 PM
To: William Hopgood <William.Hopgood@dia.govt.nz>
Cc: Julie Woods <Julie.Woods@dia.govt.nz>
Subject: RE: IVS Web Capture

Kia ora

In terms of the impact on customers, this isn't a huge change, and a beneficial one at that (given the basic agreement content for the App Store and Google Play). I suspect we can pull the new language together in a meeting.

I'm out of the office all day tomorrow, but otherwise around for the rest of the week. Calendar is pretty sparse for Thursday and Friday (not sure how I pulled that off), so drop in an hour when suits.

Ngā mihi
Kevin

From: William Hopgood
Sent: Tuesday, 5 March 2019 15:42
To: Kevin Linnane <Kevin.Linnane@dia.govt.nz>
Cc: Julie Woods <Julie.Woods@dia.govt.nz>
Subject: IVS Web Capture

Hello Kevin,

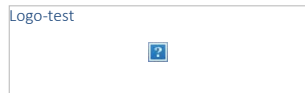
A couple of weeks ago we moved the RealMe Now App functionality on to a web based platform, meaning that customers will no longer have to download an app to do digital photo capture and can be seamlessly redirected to web capture

One thing I totally missed is the mention of digital capture on the IVS Privacy Statement:

I am hoping to modify this to be more general to the technology but I understand that most Privacy Statements require a months notice. Am I able to set a meeting to discuss:

William Hopgood | Senior Advisor
Product Development | **Te Pou Manawa**
The Department of Internal Affairs | **Te Tari Taiwhenua**
Direct Dial: +64 4 382 3576 | Extn: 4576
45 Pipitea Street, Wellington 6011, New Zealand | www.dia.govt.nz

Logo-test



Released under the Official Information Act 1982

From: [Kevin Linnane](#)
To: [Katrina Stewart](#)
Cc: [David Watson](#); [Rebecca Roper](#)
Subject: RE: Testing Images required for Passports - your help please
Attachments: [image002.png](#)

Kia ora

Sorry, I was unexpectedly out of the office for a couple of days this week. Playing catch up on half a hundred emails.

I wouldn't think an agreement or signature would be necessary for this, so long as you're very clear about why the pictures are needed and what you'll use them for (and for how long).

That said, I am working on the basis the following things are true:

- The testing database is locked down and only accessible to a small number of staff/contractors to use
- The testing database is not shared with any other agency
- The testing database does not hold any biographical information (such as names)

If this isn't the case then my below recommendation will need to be reviewed.

If posting this on 1840 I'd include the below as a footnote:

The passport sized photograph you provide will be held in the facial recognition testing database and may be used to test and improve software and systems designed for facial identification. The photograph you provide will only be available to those DIA staff members and contractors authorised to use the testing database, and will not be disclosed to other agencies. The photograph will be held in the testing database for the duration of its operation.

The testing database does not include any information beyond photographs. For this reason the photograph you provide may not be included should you make a request for personal information held by DIA unless the testing database is specified in the request. The photograph you provide can be removed from the testing database upon your request at any time.

How you shape the message around the images you want is something I'd run past comms. I'd suggest a focus on wanting to be ensure our systems are fit for purpose in an increasingly diverse and inclusive New Zealand society.

Ngā mihi
Kevin

From: Katrina Stewart
Sent: Friday, 28 September 2018 13:34
To: Kevin Linnane
Cc: David Watson; Rebecca Roper
Subject: RE: Testing Images required for Passports - your help please

Hi Kevin

Checking in to see if you could please come back to me on the below today?

Cheers

Katrina

From: Katrina Stewart
Sent: Thursday, 27 September 2018 9:37 AM
To: Kevin Linnane
Cc: David Watson; Rebecca Roper
Subject: Testing Images required for Passports - your help please
Importance: High

Kia ora Kevin

I am following up on David Watson's email below. Is it possible you could please come back to us by tomorrow afternoon?

We need to start taking photos very shortly to meet our project timeframes.

Ngā mihi
Katrina

Katrina Stewart | Workstream Lead
Uruwhenua 2020
Techonology Services and Solutions
Ngā Tohu Ratonga | Shared Services
Te Tari Taiwhenua | Department of Internal Affairs

DIA Logo - Email Signature



From: David Watson
Sent: Monday, 24 September 2018 1:07 PM
To: Hiranthi Abeygoonsekera
Cc: Kevin Linnane; Tim Whiteley
Subject: RE: Testing Images required for Passports

Thanks Hiranthi,

Hi Kevin, just to inform you this is for the Uruwhenua project.

Thanks

From: Hiranthi Abeygoonsekera
Sent: Monday, 24 September 2018 12:46 PM
To: David Watson
Cc: Kevin Linnane; Tim Whiteley
Subject: RE: Testing Images required for Passports

Hi David,

This seems like a privacy question, so I suggest you contact Kevin Linnane. I have copied Kevin into this e-mail.

Hiranthi

Hiranthi Abeygoonesekera

Chief Legal Advisor | Kāhui Kaitohu Ture

Legal Services | Ngā Ratonga Ture

The Department of Internal Affairs Te Tari Taiwhenua

Direct Dial: +64 4 4956075 | Extn: 5175 | 9(2)(a)

PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

The information contained in this email message is for the attention of the intended recipient only. If you are not the intended recipient you must not disclose, copy or distribute this message or the information in it. If you have received this message in error, please destroy the email and notify the sender immediately. This e-mail may also contain legal advice which will be legally privileged.

From: David Watson
Sent: Monday, 24 September 2018 12:42 PM
To: Hiranthi Abeygoonesekera
Subject: Testing Images required for Passports

Hi Hiranthi,

I wasn't too sure who to ask this question to.

I'm the Test manager across the passports systems, and we are needing to test a variety of images for some proof of concept checks for some passport testing.

We have many amounts of existing photo's but need to cover some quite specific scenario's.

I was wanting to post a message on the 1840 bulletin board asking for some volunteers, but was wondering if we needed something for anyone who volunteers to sign?

These images will only be used for testing, but will likely be needed for a very long time.

The scenario's we need are;

- Brown skin with fair/grey/white hair
- Black skin with fair/grey/white hair
- Black skin with dark hair

Would you be able to point me in the right direction of who I may be able to contact about this?

Kind Regards

David Watson | Test Manager | Service and System Transformation

Department of Internal Affairs Te Tari Taiwhenua

Direct Dial: +64 4 474 8180 | Extn: 8180

45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz



From: [Venkat Maddali](#)
To: [Emma Pond](#)
Cc: [Margot Brough](#); [Kevin Linnane](#)
Subject: RE: RealMe Replatforming - PIA - query re assertion service personal information
Date: Thursday, 9 January 2020 4:31:49 PM
Attachments: [image001.png](#)

Hi Emma,

The verification process is on IVS platform ^{9(2)(k)} [REDACTED]. So there wont be any verification process and data related to identity including photo wont be saved in new platform.

The new platform's RealMe assertion service is a pass through service for integrated agencies and private sector services like banks.

RealMe Now App is out of scope for this . We are not planning to move RealMe Now environment to cloud not even in near future.

Regards,
Venkat

From: ^{9(2)(a)} [REDACTED]
Sent: Thursday, 9 January 2020 3:44 PM
To: Venkat Maddali <~~x@xx~~>
Cc: Margot Brough <~~x@xx~~>; Kevin Linnane <Kevin.Linnane@dia.govt.nz>
Subject: RealMe Replatforming - PIA - query re assertion service personal information

Hi Venkat

I have a follow up questions please - not sure if you are the right person to direct it to so have copied in Margot and Kevin as well, apologies for the scattergun approach.

In terms of the assertion service, my understanding is that when someone applies to have their identity verified they complete an application process which requires them to provide DIA with certain personal information (eg from an identity document such as a passport or birth certificate). They also have to have a photo taken, and DIA may also collect personal information from other sources (such as BDM, passports, immigration) to assist in confirming their identity.

My question is where this information that is collected as part of the verification process is held. Will this information (including the photograph) be held on the new platform? If so, for how long?

Also I'm assuming that the RealMe app is out of scope for this PIA ie the personal information collected via the app (including anything related to facial recognition) is not being moved to the new platform (at this point in time)?

Hope that makes sense, happy to discuss
Cheers ^{9(2)(a)} [REDACTED]

9(2)(a)



m
p
w

9(2)(a)



The information in this email is confidential and may be legally privileged.
If you are not the intended recipient, please respect this and notify me immediately by telephone.
Please also destroy the email. Thank you.

Released under the Official Information Act 1982

From: [Privacy](#)
To: [Antonia Aloe](#); [Privacy](#)
Cc: [Peter Campbell](#); [Dale Robinson](#)
Subject: RE: Updated Facial Recognition Replacement Privacy Threshold Assessment
Attachments: [image002.png](#)
[image003.png](#)

Mōrena Antonia

For possibly the first time ever I find myself comfortable signing a recommendation to not complete a full PIA when there are identified High impacts. Document signed and ready for Russell.

I agree that the significant risks relate to Access and Secure Storage. These will be best managed through the Cloud Assessment and C&A processes.

I have no concerns about the collection, usage, or disclosure of the information. These are managed through existing processes.

There may be an outstanding risk around the retention of information, but this will require consideration of the interaction between the Public Records Act 2005 and obligations under the Passports Act 1992 to verify applicant information.

Should the Cloud Assessment and/or C&A processes identify issues which have not been considered to date the Privacy Threshold Assessment may need to be updated and a further decision made on whether a full or targeted PIA completed.

Nō reira,
Nāku iti nei,
Nā Kevin

Kevin Linnane

Kaitohutohu matua Tūmataitinga Principal Advisor Privacy
Rōpū Mōhiohio me te Haumarua Information and Safety
Te Tari Taiwhenua **Department of Internal Affairs**

Mobile 9(2)(a)

45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

Please note that I work from home on Tuesdays.

cid:image002.jpg@01D3525A.A53B5660



From: Antonia Aloe <xxxxxxx.xxxx@xxx.xxxx.xx>

Sent: Wednesday, 19 February 2020 15:21

To: Privacy <xxxxxxx@xxx.xxxx.xx>

Subject: FW: Updated Facial Recognition Replacement Privacy Threshold Assessment

Hi

For Privacy Team review and sign off.

Ngā mihi,

Antonia Aloe | Senior Project Manager |
Te Ara Matihiko | Technology Services and Solutions

Mbl: 9(2)(a)

Level 2, 45 Pipitea Square | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

Logo-test



From: Antonia Aloe

Sent: Monday, 17 February 2020 8:44 AM

To: Kevin Linnane <xxxxx.xxxxxxx@xxx.xxx.xx>

Cc: Peter Campbell <xxxxx.xxxxxxx@xxx.xxx.xx>; Dale Robinson <xxxxx.xxxxxxx@xxx.xxx.xx>

Subject: RE: Updated Facial Recognition Replacement Privacy Threshold Assessment

Kia ora Kevin

Just following up on this request and whether you have any further feedback?

Ngā mihi,
Antonia

From: Antonia Aloe

Sent: Friday, 7 February 2020 9:57 AM

To: Kevin Linnane <xxxxx.xxxxxxx@xxx.xxx.xx>

Cc: Peter Campbell <xxxxx.xxxxxxx@xxx.xxx.xx>; Dale Robinson <xxxxx.xxxxxxx@xxx.xxx.xx>

Subject: Updated Facial Recognition Replacement Privacy Threshold Assessment

Kia ora Kevin

Now that the Facial Recognition as a Service (FRaaS) design and build have been completed, we've updated the Privacy Threshold Assessment for your review, and then Russell's endorsement. [Privacy Threshold Analysis_FRaaS_Updated Feb 2020.docx](#)

Key changes:

1. FRaaS will now process youth (11-15 year old) images, image id and associated biographic data sourced from Passports systems. *Previously it was only adults (from 16 years old)*
2. Images as well as limited biographic data sourced from DIA Passports Systems will be provided and stored in FRaaS for the purposes of biometric matching. This data is limited to image id, identified gender, age at time of capture (calculated from application received date and date of birth), place of birth, country of birth and Image capture date (date application is received). *Previously it was thought only images would be provided*

and no biographic (personal information) would be provided. We have added how this data will be stored in, and used by FRaaS.

3. Updated the FRaaS and Integration with Passports diagram.

We expect the outcomes of the security and could assessment from DXC end March/ April, as this is a pre-requisite for the PTA recommendation.

This is the previously approved PTA. [FRS_PIA_TC_2017-03-21_Privacy_review.pdf](#)

Ngā mihi,

Antonia Aloe | Senior Project Manager |

Te Ara Matihiko | Technology Services and Solutions

Mbl: 9(2)(a)

Level 2, 45 Pipitea Square | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

Logo-test



Released under the Official Information Act 1982

From: [Tim Waldron](#)
To: [Fran Rigby](#); [Grant Stark](#); [Kevin Linnane](#); [Logan Fenwick](#); [Emily Redmond](#)
Cc: [Simon Millswell](#); [Ravi Casinader](#)
Subject: FW: RealMe One Time Identity Concept
Date: Thursday, 28 May 2020 4:13:30 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.jpg](#)
[OTI overview - 31 May 2019.pptx](#)
[OTI Product Overview.docx](#)

Hi Fran,

I met with OPC (Neil and Eve) on 10 June 2019. Ash Brocklebank (DIA) was also in attendance (my follow-up note to OPC below). The engagement with OPC was prior to the development of Richard's opinion.

The session was to run through the concept and work we were doing (i.e. heads up). It was undertaken as an early activity ahead of any detailed discussions around policy and privacy aspects. I'm not sure if specific follow-up happened due to (from my memory) contention around the use of Passports Act (based around Police engagement concurrently happening).

Cheers

Tim Waldron

From: Tim Waldron
Sent: Tuesday, 11 June 2019 9:53 AM
To: Neil Sanson <xxxx.xxxxxx@xxxxxxx.xxx.xx>; Eve Kennedy <Eve.Kennedy@privacy.org.nz>
Cc: Ash Brocklebank <xxx.xxxxxxxxxxxx@xxx.xxxx.xx>; Angeline Cuzens <xxxxxxxx.xxxxxx@xxx.xxxx.xx>
Subject: RealMe One Time Identity Concept

Hi Neil & Eve

Thanks for your time yesterday. It was great to have the opportunity to provide some background around progress we have made with the web photo capture and the exploration of the One Time Identity concept. As discussed, we are currently in the process of preparing a privacy impact assessment, which will look to provide to you for advice/discussion later in the month (or early August). Hopefully, the session yesterday will provide useful context for next stages of your Office's involvement.

I have attached copies of the document provided yesterday.

As noted, we have established a 'sandbox' to test of the OTI concept with prospective user agencies, with the following goals:

- To ensure it meets the business needs of potential client organisations around digital onboarding and identifying any new requirements
- To ensure it meets the needs of end users for digital on boarding.

As noted , we are also be reviewing policy, privacy and operational requirements along with the

supporting commercial model options.

If you have any questions please get in touch with either Ash or myself.

Regards

Tim Waldron | Manager, Market and Business Development | Service Innovation Te Pūnaha Matarua
Service & System Transformation (SST) Te Kōtui Whitiwhiti

Department of Internal Affairs Te Tari Taiwhenua

45 Pipitea Street, PO Box 6140, Wellington

Direct Dial: 04 382 3608 | Extn: 4608 | Mobile ^{9(2)(a)} [REDACTED] | www.dia.govt.nz

DIA black logo small



Released under the Official Information Act 1982

From: [Kevin Linnane](#)
To: [Lydia Kafatolu](#)
Subject: RE: [REDACTED] De-duplication memo
Attachments: [image004.png](#)

Kia ora Lydia

Thank you for sending this through. I was aware of the exercise but hadn't noted the potential match images would be collated outside of the Passports systems for the manual step.

I support the three month deadline for the disposal of this extracted information. These are very much transitory records with no business need for retention once the checks have been completed. ^{9(2)(k)} [REDACTED]
[REDACTED]

^{9(2)(k)} [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Enjoy your weekend and I hope this goes very smoothly.

Nō reira,
Nāku iti nei,
Nā Kevin

Kevin Linnane

Kaitohutohu matua Tūmataitinga Principal Advisor Privacy
Rōpū Mōhiohio me te Haumarua Information and Safety
Te Tari Taiwhenua Department of Internal Affairs

Mobile ^{9(2)(a)} [REDACTED]

45 Pipitea Street | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

cid:image002.jpg@01D3525A.A53B5660



From: Lydia Kafatolu
Sent: Thursday, 25 June 2020 14:45
To: Kevin Linnane
Subject: [REDACTED] De-duplication memo

[Redacted]

Kia ora Kevin,

9(2)(k) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted]
-
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

Ngā mihi

Lydia Kafatolu | Investigator | Business Services |
The Department of Internal Affairs Te Tari Taiwhenua
PO Box 1568 Wellington 6140 | www.dia.govt.nz



Released under the Official Information Act 1982

Information may be released to assist with an official investigation under Principle 11(e) of the Privacy Act 1993.

Released under the Official Information Act 1982

From: [Caroline Carver](#)
To: [David Philp](#); [Kevin Linnane](#)
Cc: [Grant Stark](#); [Antonia Aloe](#)
Subject: OTI Documents and Feedback from OPC
Date: Friday, 17 July 2020 10:45:57 PM
Attachments: [image011.jpg](#)
[image012.jpg](#)
[image013.png](#)
[image014.png](#)
[image015.png](#)
[RE: \[REDACTED\] OTI Documents for Consultation.msg](#)

Hi David/ Kevin

We have received feedback from OPC regarding the OTI (attached) which is very positive from a DIA side. You will note they haven't yet issued the final commissioner comment that we need for the finalisation of the Confirmation Agreement as MSD have not provided them the required information regarding the handling and requirement for the selfie image yet to enable this.

However we have updated our documents in accordance with their feedback and we now have the following items that can now be finalised subject to your final review.

[OTI PIA](#)

[MSD Operating Procedures](#)

Please note the following from OPC:

- We understand that MSD will utilise the OTI functionality for clients based overseas in the future – primarily, NZ Super beneficiaries. We request to be consulted on any future releases that will utilise the OTI functionality for clients based overseas.
- We recommend DIA update their privacy breach processes to reflect the Privacy Act 2020.
- We recommend that DIA undertakes a first-principles approach to review the entirety of the IICA due to how it overlaps with the Privacy Act's AISA framework.

Please let me know if you have any further comments or questions on these documents.

Regards
Caroline

Caroline Carver | Privacy Consultant
Department of Internal Affairs Te Tari Taiwhenua
Mobile: 9(2)(a) [REDACTED] | www.dia.govt.nz



From: [Caroline Carver](#)
To: [Demi Mitchell](#); [Eddie Jeffries](#)
Cc: [Michael Harrison](#); [Eve Kennedy](#); [Grant Stark](#); [Antonia Aloe](#); [Kevin Linnane](#)
Subject: RE: [REDACTED] OTI Documents for Consultation
Date: Friday, 17 July 2020 10:34:51 PM
Attachments: [image014.jpg](#)
[image015.jpg](#)
[image016.png](#)
[image001.jpg](#)
[image002.jpg](#)
[image003.png](#)
[image017.png](#)
[image018.png](#)
[Privacy Statement OTI.pdf](#)
[DIA - Privacy Impact Assessment Full - OTI.docx](#)

Hi

Thanks very much for your feedback. I have added some comments below.

Comments on the PIA

I have attached an updated PIA with track changes.

- We understand from DIA that data will only be stored in NZ, although in the unlikely event Daon need access to production data they are based in Australia. We have therefore inferred that the CLOUD Act will not apply. Can you confirm whether you agree? – **Can confirm we agree with this.**
- There is currently no Disposal Authority under the Public Records Act that explicitly details the handling of the OTI information. - This could be amended to make clearer that there is currently no process at MSD to delete OTI information, e.g. 2 years after the individual dies. – **The PIA provided by DIA does not cover the MSD actions. This sentence relates to DIA I have made it clearer.**
- A04 - Consider reducing the maximum age of a passport for young adults. – **The reason we suggested this is for young adults there facial features change a lot. Therefore there is a higher failure rate if their passport is 10 years old for example. These individuals go through the whole process and then fail at the final stage. Suggest is we reduce the passport age for this group so they are prevented from using the service up front. It wont stop fails but it will mitigate the impact.**
- We understand that MSD will utilise the OTI functionality for clients based overseas in the future – primarily, NZ Super beneficiaries. We request to be consulted on any future releases that will utilise the OTI functionality for clients based overseas. – **noted.**
- We are yet to be provided with a copy of the privacy statement. We request to be consulted on the wording of the privacy statement. – **Please find this attached.**
- We note we have been provided with the following privacy information that will be displayed to the user before the OTI tool collects any personal information:
“Your information is collected by the Department of Internal Affairs to confirm your identity. Find out how your information is managed and how you can access it in the Identity Check Privacy Statement.”
We recommend DIA strengthen the privacy information provided before any personal information is collected by the OTI tool, by explaining what information will be shared with MSD and for what purposes. For example, if MSD are going to retain the selfie, they should be explicit about this and clearly explain how the selfie will be used. – **This is included in further details. I will get the latest screen shots to you shortly. If you would like a demo please let us know.**
- We note that R10 is given an inherent risk rating of minimal in the risk assessment table on page 21 of the PIA. We believe that the consequence of an incorrect identity confirmation being provided to MSD would be greater than ‘minimal’ as if an incorrect match was to happen, this could result in identity fraud. We recommend DIA amend the inherent risk rating of ‘minimal’ to ‘medium’ given the inaccuracy rate of 5%. – **Agreed. We don’t have medium but I have moved it up one.**
- We recommend DIA update their privacy breach processes to reflect the Privacy Act 2020. – **noted. This is part of our Act preparation plans.**

Breaches under the AISA

In terms of the plan re privacy breaches section 8.4 and 8.5 apply for the operating procedures as not all security breaches will result in a privacy breach. This only applies if the information concerned is the raw data shared under the AISA. The level of raw data held before it becomes the agencies own data as they match and update is very minimal as we are moving to APIs.

However if there is a breach of the information exchanged under an AISA before it becomes an agencies own information then the agency will notify DIA in accordance with the provisions of the AISA who will then triage and notify as per DIA standard process. There is also a carve out under the operating procedures where if there is immediate or significant risk to an individual then MSD can notify them. We believe this will allow us to conform with the requirements for notifications but happy to work through this with you if you would like.

IICA

We recommend that DIA undertakes a first-principles approach to review the entirety of the IICA due to how it overlaps with the Privacy Act's AISA framework. - noted

If we can assist with anything else please let me know.

Regards
Caroline

Caroline Carver | Privacy Consultant
Department of Internal Affairs Te Tari Taiwhenua

Mobile: 9(2)(a) | www.dia.govt.nz



From: Demi Mitchell <xxxx.xxxxxxxx@xxxxxxx.xxx.xx>
Sent: Friday, 17 July 2020 2:39 PM
To: Caroline Carver <xxxxxxx.xxxxxx@xxx.xxx.xx>; Eddie Jeffries
<9(2)(a)>
Cc: Michael Harrison <xxxxxxx.xxxxxxxx@xxxxxxx.xxx.xx>; Eve Kennedy
<xxx.xxxxxxx@xxxxxxx.xxx.xx>
Subject: RE: : OTI Documents for Consultation

Kia ora Caroline and Eddie,

Thank you for jointly consulting us on the use of DIA's OTI tool by MSD. We understand the OTI tool uses facial recognition technology, passport biometric templates and an evidence of liveness check to provide remote identity verification, without applicants being required to visit an MSD office or have a RealMe Account.

The information sharing between MSD and DIA to facilitate the OTI tool is considerably complex, due to the overlaps between the Identity Information Confirmation Act, the AISA and the Privacy Act. Thank you for your assistance over the past few days as we have been trying to grasp a greater understanding of the OTI tool and the legal framework that supports information sharing. We believe this process would have been easier had the PHRaE analysis been available as we have struggled to find details on the MSD side of the OTI tool.

Nevertheless, we have reviewed the material provided and have the following feedback. Please note that you should consider the below to be 'provisional' feedback following our analysis and conversation with the Privacy Commissioner. It is not the final comment of OPC or the Privacy Commissioner as we would like additional information (detailed below).

For the most part we consider that MSD's use of the OTI tool is proportionate and will lessen the identity verification burden on individuals, but have an outstanding concern relating to the disclosure of an applicant's selfie to MSD.

Disclosure of selfie photo by DIA to MSD

We are still not convinced that the benefits of providing a copy of the selfie to MSD will outweigh the potential privacy risks of MSD having a database of selfies from clients that have used the OTI tool.

We note that MSD currently do not have a business process to collect a photo of every client. We need further evidence before being satisfied that MSD should be able to retain the selfies of clients who have used the OTI tool, especially when the retention policy outlined in the PIA does not apply to MSD.

MSD is seeking to receive and retain the selfie to assist with the verification of identity and prevention of fraud. We have the following questions on this issue:

- Please provide more detail on why MSD need to retain the selfie? Are any secondary uses/disclosures are anticipated?
- What mitigations could be put in place to alleviate potential privacy or other risks (such as misidentification or discrimination)?
- For example, what (if any) training will be provided to frontline MSD officers so that they can accurately compare the selfie with the person standing in front of them?
- Will MSD or DIA cross-check the selfies for duplicates/similarities?
- MSD retention length of the selfie will be required – this must be tied to the use of the selfie and we anticipate this would be in months, not years, but would appreciate your advice.
- What negative impacts (for individuals and for MSD) are anticipated if the selfie is not provided to MSD?

The Commissioner is unable to provide a formal (and final) comment until he receives more information on why MSD need to retain the selfie.

Feedback on material provided

We have the following feedback on the material provided.

Privacy Impact Assessment

We consider that for the most part DIA have taken a data minimisation approach to the development of the OTI tool. With the exception the selfie, the information shared with MSD appears proportionate and necessary.

We have made some minor comments in tracked changes in the attached version of the PIA. We also wanted to note the following:

- We understand that MSD will utilise the OTI functionality for clients based overseas in the future – primarily, NZ Super beneficiaries. We request to be consulted on any future releases that will utilise the OTI functionality for clients based overseas.
- We are yet to be provided with a copy of the privacy statement. We request to be consulted on the wording of the privacy statement.
- We note we have been provided with the following privacy information that will be displayed to the user before the OTI tool collects any personal information:
“Your information is collected by the Department of Internal Affairs to confirm your identity. Find out how your information is managed and how you can access it in the Identity Check Privacy Statement.”
We recommend DIA strengthen the privacy information provided before any personal information is collected by the OTI tool, by explaining what information will be shared with MSD and for what purposes. For example, if MSD are going to retain the selfie, they should be explicit about this and clearly explain how the selfie will be used.
- We note that R10 is given an inherent risk rating of minimal in the risk assessment table on page 21 of the PIA. We believe that the consequence of an incorrect identity confirmation being provided to MSD would be greater than ‘minimal’ as if an incorrect match was to happen, this could result in identity fraud. We recommend DIA amend the inherent risk rating of ‘minimal’ to ‘medium’ given the inaccuracy rate of 5%.
- We recommend DIA update their privacy breach processes to reflect the Privacy Act 2020.

Compliance with the IICA

We have reviewed the Confirmation Agreement and note it appears to include all the content required by the IICA. However, we recommend the Confirmation Agreement be updated to reflect the obligations in the Privacy Act 2020 for the avoidance of doubt. For example, the Confirmation Agreement only includes an optional privacy breach notification to OPC when this will soon be a mandatory regime.

Feedback on the Customer Nominated Services AISA Operating Procedures

We have a minor comment in tracked changes regarding how DIA intend to advise OPC of notifiable privacy breaches (see version of Operating Procedures attached).

PHRaE report by MSD

The material we have been provided is incomplete without the PHRaE report and has required a lot of follow up questions, especially to understand the information sharing with MSD.

We believe the PHRaE report will greatly assist our understanding of how MSD will use any personal information disclosed to it by DIA from the OTI tool, including the selfie.

We request we are consulted on the PHRaE report. We understand MSD anticipated this would be with our Office by the end of this week.

Review of the IICA

As noted above, the information sharing arrangement between DIA and MSD to give effect to the OTI tool is considerably complex.

The PIA recommends amendment to the ICCA to confirm applicability where the individual provides their identity information direct to DIA.

We recommend that DIA undertakes a first-principles approach to review the entirety of the IICA due to how it overlaps with the Privacy Act's AISA framework.

Please note that I will be on annual leave next week and Eve is on annual leave until Wednesday, so Michael Harrison will be your first point of contact – apologies for this inconvenience.



Please let us know if you have any questions. We look forward to hearing from you.

Ngā mihi

Demi Mitchell, Policy Advisor

Office of the Privacy Commissioner Te Mana Matapono Matatapu
PO Box 10094, The Terrace, Wellington 6143
Level 8, 109 Featherston Street, Wellington, New Zealand
privacy.org.nz



Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.   Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From: Eddie Jeffries <[REDACTED]>

Sent: Thursday, 16 July 2020 4:16 pm

To: Demi Mitchell <Demi.Mitchell@privacy.org.nz>

Cc: Michael Harrison <Michael.Harrison@privacy.org.nz>; Caroline Carver <Caroline.Carver@dia.govt.nz>

Subject: RE: [REDACTED]: OTI Documents for Consultation

Hi Demi

Yes, Caroline is correct. The selfie is used to verify a client's identity when they visit a Service Centre.

We currently do not have a business process to collect a photo of every client. But we do scan their identity documents into our client management system. So if they use a photo ID, we will have that photo on record.

You're correct that we could ask the client security questions like, what's your DOB and address. However this is not a water tight method to verify the individual's identity. There's a risk a fraudster could obtain enough information to impersonate someone and answer these questions.

The photo provides a very robust measure to verify the individual's identity, which lowers the risk of identity fraud. It also create a more seamless service because the staff member does not need to ask the client security questions.

Happy to discuss further.
Eddie

Eddie Jeffries

Senior Advisor | Information Privacy & Sharing

9(2)(a)

Ministry of Social Development

Manaaki Tangata Manaaki Whānau

From: Demi Mitchell <xxxx.xxxxxxxx@xxxxxx.xxx.xx>

Sent: Thursday, 16 July 2020 3:47 PM

To: Eddie Jeffries 9(2)(a)

Cc: Michael Harrison <xxxxxx.xxxxxxxx@xxxxxx.xxx.xx>; Caroline Carver <xxxxxx.xxxxxx@xxx.xxx.xx>

Subject: RE: [REDACTED] OTI Documents for Consultation

Hi Eddie

Caroline has advised me that a user's selfie is shared by DIA with MSD for customer services purposes, i.e. to help MSD identify a person if they come into an MSD office.

Are you able to please expand on the reasoning behind this? As far as we understand, MSD does not keep photos of applicants currently on file, so this would mean MSD would only have photos of applicants who have gone through the OTI tool. We are having difficulty understanding why MSD would need the photo to identify a person when they come into an MSD office, as they will have to provide their DOB, etc. to confirm their identity anyway?

I look forward to your response.

Ngā mihi

Demi Mitchell, Policy Advisor

Office of the Privacy Commissioner Te Mana Matapono Matatapu

PO Box 10094, The Terrace, Wellington 6143

Level 8, 109 Featherston Street, Wellington, New Zealand

privacy.org.nz



Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to

our newsletter or follow us online.   Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From: Eddie Jeffries ^{9(2)(a)}
Sent: Thursday, 16 July 2020 9:25 am
To: Demi Mitchell <Demi.Mitchell@privacy.org.nz>
Cc: Michael Harrison <Michael.Harrison@privacy.org.nz>; Caroline Carver <Caroline.Carver@dia.govt.nz>
Subject: RE: [REDACTED]: OTI Documents for Consultation

Hi Demi

In regards to the OTI information MSD collects from DIA. I'm applying MSD's new Disposal Authority (DA) which is expected to come into force in the next year and applies to the OTI information MSD collects. This requires:

- the information to be retained for 2 years after the individual dies, then deleted; or
- if the individual updates their identity information with MSD, MSD can delete the original information it received from DIA.

Currently there is no process at MSD to delete the OTI information 2 years after the individual dies. However, once the DA comes into force the Information Management Team is planning to develop a Ministry wide deletion process of client records in-line with the DA. This will include the deletion of the OTI information 2 years after the individual dies.

I'm also working with our tech team to try set up an automatic process that deletes original identity documents when they're updated with new ones. If this is not possible in the short term, then this process will fall under the Information Management Team's work described above.

Thanks

Eddie

Eddie Jeffries

Senior Advisor | Information Privacy & Sharing



Ministry of Social Development

Manaaki Tangata Manaaki Whānau

From: Demi Mitchell <xxxx.xxxxxxx@xxxxxx.xxx.xx>
Sent: Thursday, 16 July 2020 8:33 AM
To: Caroline Carver <xxxxxx.xxxxxx@xxx.xxx.xx>
Cc: Michael Harrison <xxxxxx.xxxxxxx@xxxxxx.xxx.xx>; Eddie Jeffries
9(2)(a) [REDACTED]
Subject: RE: [REDACTED]: OTI Documents for Consultation

Great, thanks Caroline.

Eddie, I look forward to your response.

Thanks

Demi

From: Caroline Carver <xxxxxx.xxxxxx@xxx.xxx.xx>
Sent: Wednesday, 15 July 2020 6:03 pm
To: Demi Mitchell <xxxx.xxxxxxx@xxxxxx.xxx.xx>
Cc: Michael Harrison <xxxxxx.xxxxxxx@xxxxxx.xxx.xx>; Eddie Jeffries
9(2)(a) [REDACTED]
Subject: Re: [REDACTED]: OTI Documents for Consultation

Hi

The information is held by DIA within the Daon solution. This is hosted by DIA not Daon. We keep the information the person provided and the outcome of the matches etc for 6 months.

In terms of MSD retention I believe this is indefinite but have copied in Eddie for confirmation.

Regards

Caroline

Sent from my iPhone

On 15/07/2020, at 3:56 PM, Demi Mitchell <xxxx.xxxxxxx@xxxxxx.xxx.xx> wrote:

Hi Caroline

I note in the PIA that information relating to a selfie and liveness check shared with MSD will be retained for six months within the Daon solution.

Does this mean all the information MSD receives is stored in the Daon solution? i.e. full name, date of birth, confirmation of liveness and passport match and selfy.

If not, how long does MSD retain the information it receives from DIA?

Thanks in advance again!

From: Caroline Carver <xxxxxxx.xxxxxx@xxx.xxx.xx>
Sent: Wednesday, 15 July 2020 11:05 am
To: Demi Mitchell <xxxx.xxxxxxxx@xxxxxxx.xxx.xx>
Cc: Michael Harrison <xxxxxxx.xxxxxxxx@xxxxxxx.xxx.xx>
Subject: Re: [REDACTED]: OTI Documents for Consultation

Hi

That is correct.

Caroline

Sent from my iPhone

On 15/07/2020, at 11:03 AM, Demi Mitchell
<xxxx.xxxxxxxx@xxxxxxx.xxx.xx> wrote:

Thank you – one further question

In the PIA it says on p.7 that under the current system, people are required to provide two different documents that support their identity.

From our conversation, I understand that if a person doesn't have a passport, and completes selfy/liveness check, they only have to provide one form of identity in person at MSD. Is that because the selfy/liveness check serve as a form of identity?

From: Caroline Carver <xxxxxxx.xxxxxx@xxx.xxx.xx>
Sent: Wednesday, 15 July 2020 10:53 am
To: Demi Mitchell <xxxx.xxxxxxxx@xxxxxxx.xxx.xx>
Cc: Michael Harrison <xxxxxxx.xxxxxxxx@xxxxxxx.xxx.xx>
Subject: Re: [REDACTED]: OTI Documents for Consultation

Hi

Please see below.

Caroline

Sent from my iPhone

On 15/07/2020, at 10:49 AM, Demi Mitchell

<xxxx.xxxxxxx@xxxxxx.xxx.xx> wrote:

Hi Caroline

Do you mean confirmation of liveness? What is a confirmation of licenses? We state they passed the liveness check.

Does the below correctly reflect our conversation this morning:

DIA are to provide MSD with the following information:

- person's full name, date of birth – to confirm they are who they say they are (as they are directed to DIA, MSD would not already have this information unless it is shared with them by DIA) - correct where a passport check is done.
- fact passport has matched – to confirm they are the person in the passport and identity has been verified - correct
- selfy photo – for customer support (although MSD don't see the person initially when they are using the OTI tool, the selfy helps MSD identify a person if they come into an MSD office. Hopefully this will never have to be used.) - correct.
- confirmation of liveness – to confirm the person is alive (DIA do not share the liveness video).- correct.

Thanks

Demi

From: Caroline Carver <xxxxxx.xxxxxx@xxx.xxx.xx>

Sent: Wednesday, 15 July 2020 10:45 am

To: Demi Mitchell <xxxx.xxxxxxx@xxxxxx.xxx.xx>

Cc: Michael Harrison <xxxxxx.xxxxxxx@xxxxxx.xxx.xx>

Subject: Re: [REDACTED]: OTI Documents for Consultation

Hi

Sorry that should read confirmation of licenses. We don't share the liveness video.

Regards
Caroline

Sent from my iPhone

On 15/07/2020, at 10:38 AM, Demi Mitchell <xxxx.xxxxxxx@xxxxxx.xxx.xx> wrote:

Hi Caroline

Thanks so much for taking the time to speak with me on the phone.

The reason I was getting confused about what information would be passed to MSD, was because at page 4 of the PIA it says:

If the selfie and the liveness check are completed successfully and relate to the same individual, then the details are compared to the client-provided passport details. If the passport details including the passport photo match the information provided, then the client is asked to authorise the disclosure of their full name, date of birth, **liveness** and passport photo match confirmation and the selfie photo to MSD. This disclosure is authorised under the Identity Information Confirmation Act.

Can you please confirm that liveness is not shared with MSD (this was my understanding of our conversation on the phone, but the PIA seems to say it is shared).

Thanks again for your help

Demi

From: Caroline Carver
<xxxxxx.xxxxx@xxx.xxx.xx>

Sent: Wednesday, 15 July 2020 8:57 am

To: Demi Mitchell

<xxxx.xxxxxxx@xxxxxx.xxx.xx>

Cc: Michael Harrison

<xxxxxx.xxxxxxx@xxxxxx.xxx.xx>; Eve Kennedy <xxx.xxxxxxx@xxxxxx.xxx.xx>

Subject: Re: [REDACTED]: OTI Documents for Consultation

Hi

Absolutely no problem. Can you advise your phone number please.

Caroline

Sent from my iPhone

On 15/07/2020, at 8:52 AM,
Demi Mitchell
<xxxx.xxxxxxx@xxxxxx.xxx.xx>
wrote:

Thanks, Caroline.

Would you be free for a quick call this morning?

I have a few questions that might be easier dealt with over the phone.

Regards

Demi

From: Caroline Carver
<xxxxxx.xxxxxxx@xxx.xxx.xx>
Sent: Tuesday, 14 July 2020
3:00 pm
To: Demi Mitchell
<xxxx.xxxxxxx@xxxxxx.xxx.xx>
Cc: Michael Harrison
<xxxxxx.xxxxxxx@xxxxxx.xxx.xx>;
Eve Kennedy
<xxx.xxxxxxx@xxxxxx.xxx.xx>
Subject: Re: [REDACTED]: OTI Documents for Consultation

Hi

Released under the Official Information Act 1982

I can confirm that
understanding is correct.

Regards
Caroline

Sent from my iPhone

On 14/07/2020,
at 1:28 PM, Demi
Mitchell

<xxxx.xxxxxxxx@xxxxxxx.xxx.xx>

wrote:

Hi Caroline

Was great to
meet you in
person last
week.

Eve is going on
annual leave
this afternoon
so I will be your
main point of
contact for the
rest of the
week.

In respect of
One Time
Identity, could
you please
confirm my
understanding
of the following
is correct:

- When a
person
provides
their
passport
information
and a
selfie,
and a
completeness

of a
liveness
check,
they do
not need
to
provide
another
form of
ID to
MSD to
gain
access to
services.

- When a
person
does not
have a
passport,
so
cannot
provide
this
information,
but
provides
a selfie
and does
a
liveness
check,
they
need to
visit an
MSD
office
and
provide
another
form of
ID before
they can
gain
access to
services,
or have a
RealMe
Account.

Released under the Official Information Act 1982

Thanks for your
time in
advance,

Demi

From: Caroline
Carver

<xxxxxxx.xxxxxx@xxx.xxx.xx>

Sent: Monday,
13 July 2020 2:00
pm

To: Eve Kennedy

<xxx.xxxxxx@xxxxxxx.xxx.xx>


Cc: Demi
Mitchell

<xxxx.xxxxxxxx@xxxxxxx.xxx.xx>;

Michael Harrison

<xxxxxxx.xxxxxxxx@xxxxxxx.xxx.xx>

Subject: Re:

 OTI
Documents for
Consultation

Hi

There will be no
fees paid under
the IICA
component or
the AISA.
However fees
will be payable
under the MOU
for the end to
end services.

Caroline

Sent from my
iPhone

On
13/07/2020,

Released under the Official Information Act 1982

at
1:44
PM,
Eve
Kennedy
<xxx.xxxxxxx@xxxxxxx.xxx.xx>
wrote:

Hi
Caroline,

I
have
a
further
question
if
you
don't
mind.
The
PIA
refers
to
MSD
receiving
metadata
and
transaction
IDs
for
reconciling
with
billing
information,
and
there
is a
description
of
disclosing
information
for
billing
purposes.
Could
you
please
elaborate
on
this,
as

Released under the Official Information Act 1982

the
IICA
Agreement
notes
no
fees
will
be
paid?

Thanks

Eve

**Eve
Kennedy,
Policy
Adviser**

Office of the Privacy

Commissioner Te Mana

Matapono Matatapu

PO Box 10094, The Terrace,

Wellington 6143

Level 8, 109 Featherston

Street, Wellington, New

Zealand

T 04 494 7141 DDI

E xxx.xxxxxxx@xxxxxxx.xxx.xx

privacy.org.nz

<image001.jpg>

Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.

[<image002.jpg>](#)

[<image003.png>](#)

Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From:

Eve

Kennedy

Sent:

Friday,
10
July
2020
12:05
pm

To:

'Caroline
Carver'

<xxxxxxxx.xxxxxx@xxx.xxx.xx>;

Demi

Mitchell

<xxxx.xxxxxxx@xxxxxxxx.xxx.xx>

Cc:

Michael

Harrison

<xxxxxx.xxxxxxxxx@xxxxxxxx.xxx.xx>;

Grant

Stark

<xxxxx.xxxxx@xxx.xxx.xx>;

Antonia

Aloe

<xxxxxx.xxxx@xxx.xxx.xx>;

Simon

Millswell

<xxxx.xxxxxxxxx@xxx.xxx.xx>;

Kevin

Linnane

<xxxx.xxxxxxx@xxx.xxx.xx>;

Logan

Fenwick

<xxxxx.xxxxxxx@xxx.xxx.xx>;

Eddie

Jeffries

9(2)(a)

Megan

Barnes

9(2)(a)

Subject:

RE:

[REDACTED]:

OTI

Documents

for

Consultation

Thanks

Caroline.

Follow

Released under the Official Information Act 1982

up
questions:

- As far as I am aware, we have not seen the PIA for OTI. Was it completed prior to implementation of the OTI system? It would be great if you could provide this to us.

- When you say "Daon do not have access **by default** to

Released under the Official Information Act 1982

the
information”,
can
you
confirm
when
they
would
have
access
to
the
information,
the
purposes
for
which
they
will
get
access,
and
whether
they
will
store
data
outside
of
Datacom
if
this
occurs?

I
gave
you
a
call
earlier
to
discuss
the
above
– if
you'd
like
to
call
me

Released under the Official Information Act 1982

back
I'm
free
between
2
and
5pm
today.

Thanks
Eve

**Eve
Kennedy,
Policy
Adviser**

Office of the Privacy

Commissioner Te Mana

Matapono Matatapu

PO Box 10094, The Terrace,

Wellington 6143

Level 8, 109 Featherston

Street, Wellington, New

Zealand

T 04 494 7141 DDI

E xxx.xxxxxx@xxxxxxx.xxx.xx

privacy.org.nz

<image001.jpg>

Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.

[<image002.jpg>](#)

[<image003.png>](#)

Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From:

Caroline

Carver

<xxxxxxx.xxxxxx@xxx.xxx.xx>

Sent:

Thursday,

9

July
2020
5:05
pm

To:

Eve
Kennedy

<xxx.xxxxxxx@xxxxxxx.xxx.xx>;

Demi
Mitchell

<xxxx.xxxxxxxx@xxxxxxx.xxx.xx>

Cc:

Michael
Harrison

<xxxxxxx.xxxxxxxx@xxxxxxx.xxx.xx>;

Grant
Stark

<xxxxx.xxxxx@xxx.xxx.xx>;

Antonia
Aloe

<xxxxxxx.xxxx@xxx.xxx.xx>;

Simon
Millswell

<xxxxx.xxxxxxxx@xxx.xxx.xx>;

Kevin
Linnane

<xxxxx.xxxxxxxx@xxx.xxx.xx>;

Logan
Fenwick

<xxxxx.xxxxxxxx@xxx.xxx.xx>;

Eddie
Jeffries

9(2)(a)

Megan
Barnes

9(2)(b)(i)

Subject:

RE:

[REDACTED]:

OTI
Documents
for
Consultation

Hi

Thanks
for
your

Released under the Official Information Act 1982

email.
Please
see
comments
below.

Regards
Caroline

**Caroline
Carver**

|
Privacy
Consultant

**Department
of
Internal
Affairs**

**Te
Tari
Taiwhenua**

Mobile:

9(2)
(a)

|

|
www.dia.govt.nz

<image004.jpg>

<image005.jpg>

<image006.png>

<image007.png>

<image008.png>

From:

Eve
Kennedy

<xxx.xxxxxxx@xxxxxxx.xxx.xx>

Sent:

Thursday,
9
July
2020
4:50
PM

To:

Caroline

Carver

<XXXXXXXX.XXXXXX@XXX.XXXX.XX>;

Demi

Mitchell

<XXXX.XXXXXXXXXX@XXXXXXXX.XXX.XX>

Cc:

Michael

Harrison

<XXXXXXXX.XXXXXXXXXX@XXXXXXXX.XXX.XX>;

Grant

Stark

<XXXXX.XXXXXX@XXX.XXXX.XX>;

Antonia

Aloe

<XXXXXXXX.XXXX@XXX.XXXX.XX>;

Simon

Millswell

<XXXXX.XXXXXXXXXX@XXX.XXXX.XX>;

Kevin

Linnane

<XXXXX.XXXXXXXXXX@XXX.XXXX.XX>;

Logan

Fenwick

<XXXXX.XXXXXXXXXX@XXX.XXXX.XX>;

Eddie

Jeffries

9(2)(a)

Megan

Barnes

9(2)(b)(i)

Subject:

RE:

[REDACTED]:

OTI

Documents

for

Consultation

Hi

Caroline,

Thanks

for

the

attached.

We

have

Released under the Official Information Act 1982

a
couple
of
questions
having
reviewed
the
PIA.
Having
not
received
more
details
information
about
OTI
since
a
short
briefing
in
June
last
year,
I
have
approached
the
PIA
as
though
it
pertains
to
the
OTI
solution
as
a
whole,
as
well
as
MSD's
use
of
OTI.
Could
you
confirm
with
me
for
the

Released under the Official Information Act 1982

avoidance
of
doubt
whether
DIA
is
already
using
OTI
for
its
own
business
processes?

We
do
already
use
the
OTI
in a
form
for
DIA
operations.
However
this
is
subject
to
a
separate
PIA.
This
PIA
and
consultation
is
just
about
the
use
of
OTI
for
MSD.

Could
you
please
provide
some
more
detail

Released under the Official Information Act 1982

about
the
arrangement
with
Daon?
Are
they
storing
information
on
behalf
of
DIA
or
processing
it?
Is
that
in
NZ
or
offshore?

They
provide
software
as
a
service
that
runs
on
DIA
infrastructure
using
data
held
by
DIA
at
Datacom
NZ.
Daon
don't
have
access
by
default
to
the
information
concerned.

I
read
13.1

Released under the Official Information Act 1982

and
13.4
as
indicating
that
Daon
will
store
information
on
behalf
of
DIA,
but
it is
unclear
where
the
“Daon
solution”
is
located
and
how
it
relates
to
DIA
systems.

I
also
note
that
at
10.2,
the
PIA
indicates
that
the
algorithm
has
been
improved
since
testing
in
2019
indicated
a
false
negative
rate

Released under the Official Information Act 1982

of
less
than
5%.
Could
you
advise
how
the
algorithm
has
been
improved,
and
how
Daon
know
it
has
been
improved
if
testing
data
is
not
available?

The
algorithm
is
used
by
many
customers
not
just
DIA.
They
have
worked
with
their
own
test
datasets
and
other
customers
to
improve
the
algorithm.
The
indication

Released under the Official Information Act 1982

from
feedback
from
Daon
is it
is
improved
but
they
could
provide
no
formal
evidence
at
this
stage.

With
regards
to
the
metadata,
it
appears
that
there
will
be
personal
information
involved
as
MSD
will
be
able
to
identify
what
client
is
involved.
Could
you
please
confirm
what
you
mean
by
"Privacy
Act

—

Released under the Official Information Act 1982

Detailed
disclosure”
at
11.1
as
the
legal
basis
for
disclosure?

In
reference
to
this
we
are
talking
about
a
disclosure
we
have
made
the
customer
aware
of
as
part
of
the
privacy
statement
that
the
individual
has
authorised
by
choosing
to
use
the
service
and
is
related
to
the
purpose
of
the
service.

Released under the Official Information Act 1982

MSD
–
could
you
please
advise
whether
you
intend
to
provide
a
PHRaE
assessment
to
us,
and
if
so,
when
we
might
expect
it?

A
PHRaE
is
expected
to
be
made
available.
Eddie
will
be
able
to
confirm
the
expected
date.

Thanks
very
much

Eve

Eve
Kennedy,
Policy
Adviser
Office of the Privacy
Commissioner Te Mana

Released under the Official Information Act 1982

Matapono Matatapu
PO Box 10094, The Terrace,
Wellington 6143
Level 8, 109 Featherston
Street, Wellington, New
Zealand
T 04 494 7141 DDI

E xxx.xxxxxxx@xxxxxxx.xxx.xx

privacy.org.nz

<image001.jpg>

Privacy is about protecting personal information, yours and others. To find out how, and to stay informed, [subscribe](#) to our newsletter or follow us online.

[<image002.jpg>](#)

[<image003.png>](#)

Have a privacy question? [AskUs](#)

Caution: If you have received this message in error please notify the sender immediately and delete this message along with any attachments. Please treat the contents of this message as private and confidential. Thank you.

From:

Caroline
Carver

[<xxxxxxx.xxxxxx@xxx.xxx.xx>](mailto:xxxxxxx.xxxxxx@xxx.xxx.xx)

Sent:

Tuesday,
30
June
2020
5:09
pm

To:

Eve
Kennedy

[<xxx.xxxxxxx@xxxxxxx.xxx.xx>](mailto:xxx.xxxxxxx@xxxxxxx.xxx.xx);

Demi
Mitchell

[<xxxx.xxxxxxx@xxxxxxx.xxx.xx>](mailto:xxxx.xxxxxxx@xxxxxxx.xxx.xx)

Cc:

Michael
Harrison

[<xxxxxxx.xxxxxxx@xxxxxxx.xxx.xx>](mailto:xxxxxxx.xxxxxxx@xxxxxxx.xxx.xx);

Grant

Stark

<xxxxx.xxxxx@xxx.xxx.xx>;

Antonia

Aloe

<xxxxxxx.xxxx@xxx.xxx.xx>;

Simon

Millswell

<xxxxx.xxxxxxxxx@xxx.xxx.xx>;

Kevin

Linnane

<xxxxx.xxxxxxxx@xxx.xxx.xx>;

Logan

Fenwick

<xxxxx.xxxxxxxx@xxx.xxx.xx>;

Eddie

Jeffries

9(2)(a)

Megan

Barnes

9(2)(a)

Subject:

[REDACTED]:

OTI

Documents

for

Consultation

Hi

Eve

/

Demi

As

per

my

previous

email

please

find

attached

the

following

draft

documents

relating

to

the

One

Released under the Official Information Act 1982

Time
Identity
Project
with
MSD
for
consultation:

- DIA
PIA
for
One
Time
Identity
–
this
is
up
to
and
including
the
disclosure
to
MSD
- Confirmation
Agreement
–
to
allow
confirmation
of
passport
information
- Operating
Procedures
–
to
support
manual
checks
of
passport
information

The
MSD
PHRaE
report

Released under the Official Information Act 1982

is
still
a
couple
days
off
being
ready,
so
instead
please
find
attached
a
description
of
how
MSD
will
use
the
information
it
receives
from
DIA.

We
look
forward
to
discussing
these
documents
further
with
you
after
your
review.

Regards
Caroline

**Caroline
Carver**
|
[Privacy](#)
[Consultant](#)

Released under the Official Information Act 1982

Department
of
Internal
Affairs
Te
Tari
Taiwhenua

Mobile:

SEE
MAI
L



www.dia.govt.nz

<image009.jpg>

<image010.jpg>

<image011.png>

<image012.png>

<image013.png>

----- This email and any attachments may contain information that is confidential and subject to legal privilege. If you are not the intended recipient, any use, dissemination, distribution or duplication of this email and attachments is prohibited. If you have received this email in error please notify the author immediately and erase all copies of the email and attachments. The Ministry of Social Development accepts no responsibility for changes made to this message or attachments after transmission from the Ministry. -----

----- This email and any attachments may contain information that is confidential and subject to legal privilege. If you are not the intended recipient, any use, dissemination, distribution or duplication of this email and attachments is prohibited. If you have received this email in error please notify the author immediately and erase all copies of the email and attachments. The Ministry of Social Development accepts no responsibility for changes made to this message or attachments after transmission from the Ministry. -----

Released under the Official Information Act 1982

From: [Kevin Linnane](#)
To: [Antonia Aloe](#)
Cc: [Dale Robinson](#)
Subject: RE: FRaaS - DXC Proposal for Security Data going offshore
Attachments: [image001.png](#)
[FRS_PIA_TC_2017-03-21_Privacy_review.pdf](#)

Kia ora Antonia

Apologies for the delay. I'm going away after Easter and trying to get a thousand things done before I go.

I've read over the Threshold assessment and made some changes (attached). Specifically the sensitivity of the information has been marked up to High, and the significance of the change is Medium.

The increase to High is because of the volume of information, and the fact that if biometric data is compromised, it can never be fixed for the individual. The significance rating is standard. Any introduction of a new tool hits that as a minimum.

Whilst these are changes to the assessment, I am still accepting the recommendation.

The risks are primarily security based, with a couple of exceptions listed below that will need to be managed by the business.

Providing the security assessment is completed and doesn't identify any significant (Tier 1 or 2) risks, this should be able to proceed to deployment without any interference with individual privacy.

Questions for DXC

1. What information will be held where?

Their documents so far indicate it will be system logs, which doesn't include DIA customer information

2. Where is the datacentre?

There are some countries I am happy to hold data in. There are some we really aren't.

We need a physical location and the redundancy locations they use.

These are essential factors when considering privacy risk.

Several countries have very territorial laws that would provide them access to data held within their jurisdiction.

In shorthand, Australia and Europe are fine, the USA and Canada generally are, but we'll want to check the terms. Anywhere else gets tricky.

As far as handing back to the business goes, there needs to be a human check before the matched data is used to support a decision.

Algorithmic transparency is a big focus for this Cabinet and the SSC. We need to ensure that any computer decision is verified by a person.

I've copied Dale in as he'll likely get the job of watching this for privacy risks whilst I'm away. If things start to look risky, bring in Marie (who knows my stable of contractors).

Ngā mihi
Kevin

From: Antonia Aloe
Sent: Tuesday, 16 April 2019 09:07
To: Kevin Linnane <xxxxx.xxxxxxx@xxx.xxx.xx>
Subject: RE: FRaaS - DXC Proposal for Security Data going offshore

Hi Kevin

Would you have some time to review this request I sent through to you last week?

Kind regards,
Antonia

From: Antonia Aloe
Sent: Wednesday, 10 April 2019 8:32 AM
To: Kevin Linnane <xxxxx.xxxxxxx@xxx.xxx.xx>
Subject: FW: FRaaS - DXC Proposal for Security Data going offshore

Hi Kevin

Dale Robinson suggested I forward this to question to the Privacy Team. DIA has engaged DXC to provide Facial Recognition as a Service to replace the current FR system used by the Passports System. We're currently in the design phase. DXC have sent me a request seeking approval to send offshore some of the data used by various DXC Security Services as part of the FRaaS Service: [Security Services Data.docx](#)

Section 16.3 of the FR Services MSA doesn't permit the Service Provider to transfer, store or make available to any person any Data outside New Zealand, unless expressly authorised by the Lead Agency in writing. DIA is the Lead Agency.

Dale has provided me with his feedback and brief assessment from a Security perspective and what he would expect/ require of DXC to give us confidence around security management of this data going offshore?

Would you be able to review this from a privacy perspective and any privacy related controls you'd expect of DXC?

I've attached the initial Privacy Impact Assessment conducted.

Kind regards, Antonia

Antonia Aloe | Senior Project Manager | Technology Services and Solutions

The Department of Internal Affairs Te Tari Taiwhenua

Mbl: 9(2)(a)

Level 2, 45 Pipitea Square | PO Box 805, Wellington 6140, New Zealand | www.dia.govt.nz

Planned leave: 19-26 April, 24-28 June.



From: Dale Robinson

Sent: Tuesday, 9 April 2019 1:13 PM

To: Antonia Aloe <xxxxxxx.xxxx@xxx.xxxx.xx>; John Crawford-Smith <John.Crawford-xxxxx@xxx.xxxx.xx>

Cc: Jadrah Tupai <xxxxxxx.xxxxxx@xxx.xxxx.xx>; Peter Campbell <xxxxx.xxxxxxxx@xxx.xxxx.xx>; Esther Williams <xxxxxxx.xxxxxxxx@xxx.xxxx.xx>

Subject: RE: FRaaS - DXC Proposal for Security Data going offshore

Sorry, one thing further. It could be an appropriate step to actually audit the controls in place around where the SIEM actually is. This could be through our own security assurance processes to review and evaluate provided documentation for the service.

Dale

From: Dale Robinson

Sent: Tuesday, 9 April 2019 1:11 PM

To: Antonia Aloe <xxxxxxx.xxxx@xxx.xxxx.xx>; John Crawford-Smith <John.Crawford-xxxxx@xxx.xxxx.xx>

Cc: Jadrah Tupai <xxxxxxx.xxxxxx@xxx.xxxx.xx>; Peter Campbell <xxxxx.xxxxxxxx@xxx.xxxx.xx>; Esther Williams <xxxxxxx.xxxxxxxx@xxx.xxxx.xx>

Subject: RE: FRaaS - DXC Proposal for Security Data going offshore

Hi,

Can I suggest that this question is also forwarded across to those in the privacy team? E.g. Sue Boland-Vernon, Caroline Carver.

My notes:

9(2)(k)

[Redacted content]

All the best,
Dale

From: Antonia Aloe
Sent: Monday, 8 April 2019 1:31 PM
To: Dale Robinson <xxxx.xxxxxxxx@xxx.xxx.xx>; John Crawford-Smith <John.Crawford-xxxxx@xxx.xxxx.xx>
Cc: Jdrah Tupai <xxxxxx.xxxxx@xxx.xxx.xx>; Peter Campbell <xxxxxx.xxxxxxxx@xxx.xxx.xx>; Esther Williams <xxxxxx.xxxxxxxx@xxx.xxx.xx>
Subject: FW: FRaaS - DXC Proposal for Security Data going offshore

Hi Dale & John

DXC have sent me a request seeking approval to send offshore some of the data used by various DXC Security Services as part of the FRaaS Service.

Section 16.3 of the FR Services MSA doesn't permit the Service Provider to transfer, store or make available to any person any Data outside New Zealand, unless expressly authorised by the Lead Agency in writing.

Dale, would you mind assessing the attached description of the Security Data that DXC would like to transfer/store offshore? What would we require of them to give us confidence around security management of this data? Let me know if you require further information from DXC.

John, would it be you/ Russell that would give the approval to the request, or with conditions?

Regards, Antonia

From: Macquarrie, Tracey <xxxxxx.xxxxxxxx@xxx.xxx>
Sent: Monday, 8 April 2019 12:43 PM
To: Antonia Aloe <xxxxxx.xxxx@xxx.xxxx.xx>
Cc: Andrews, Clayton <xxxxxx.xxxxxxxx@xxx.xxx>; Greer, David <xxxxxx@xxx.xxx>; McVey,

Released under the Official Information Act 1982

Kevin <xxxxx.xxxxx@xxx.xxx>; Lintott, Sharon <xxxxxx.xxxxxxx@xxx.xxx>

Subject: Security Data going offshore

Morning Antonia

As per our discussion this morning, attached is a description of the Security Data that will be going offshore as part of the FRaaS solution.

Happy to meet and discuss with your security/architectural people if necessary.

Would like confirmation from DIA that this approach is acceptable.

Rgds

Tracey Macquarrie
Programme/Project Manager

M ^{9(2)(a)}

DXC Technology
8 Gilmer Terrace
Wellington

[dxc.technology](#) / [Twitter](#) / [Facebook](#) / [LinkedIn](#)

DXC Technology Company -- This message is transmitted to you by or on behalf of DXC Technology Company or one of its affiliates. It is intended exclusively for the addressee. The substance of this message, along with any attachments, may contain proprietary, confidential or privileged information or information that is otherwise legally exempt from disclosure. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient of this message, you are not authorized to read, print, retain, copy or disseminate any part of this message. If you have received this message in error, please destroy and delete all copies and notify the sender by return e-mail. Regardless of content, this e-mail shall not operate to bind DXC Technology Company or any of its affiliates to any order or other contract unless pursuant to explicit written agreement or government initiative expressly permitting the use of e-mail for such purpose. --.

Released under the Official Information Act 1982