Te Tari Pūreke
Firearms Safety Authority

11 May 2024

IR-01-24-16550

s 9(2)(a) OIA

Tēnā koe s 9(2)(a) OIA

Thank you for your Official Information Act 1982 (OIA) requests dated 14 May 2024 where you submitted three requests in relation to the Firearms Registry and data security.

Te Tari Pūreke – Firearms Safety Authority has consolidated these three requests into one response, and each is answered below.

1. *Could the NZ Police please provide the definition of "uplift" as used by the NZ Police and any legal definition(s) / advice they have with how that word is to be used.*

There is no document recording a definition nor legal advice regarding any definitions of the word “uplift”. Therefore, this part of your request is refused under section 18(e) of the OIA as the information requested does not exist.

2. *Could the NZ Police please confirm all the valid ways to inform the Police / Firearms Safety Authority of any new / updated information.*

   From Regulation 37(1) of the Arms Regulations 1992:

   "Except as otherwise provided in the Act or these regulations, information that the Act or these regulations require to be provided to the Police for the purposes of entry in the registry must be provided in a manner or form determined by the Commissioner."

   Can you please provide the full list of "manner" and "form" that have been determined by the Commissioner. This must include the document(s) which list the methods and all legal advice to confirm the alignment with the all applicable NZ legislation.

   Can you also provide the method(s) by which this information is easily accessible to any person with a firearms licence, e.g. a URL on the Police / Firearms Safety Authority website.

   Can you confirm the publication date(s) (or similar as applicable to the method of publication).

This part of your request has been interpreted as being in relation to the Firearms Registry.

As outlined on Te Tari Pūreke’s website under *How to register or update your information*, information for the Registry can be provided online through MyFirearms, or via Freephone: 0800 844 431 (within New Zealand) or +64 4 499 2870 (if you are not in New Zealand). Please refer to the below website link:

https://www.firearmssafetyauthority.govt.nz/firearms-registry/how-register-or-update-your-information

3. *The NZ Police Firearms Safety Authority goes into a significant level of detail about the security of data it holds on the following page of their website:*

   About the Firearms Registry | Firearms Safety Authority New Zealand
   Example text includes:
   ** "These are similar controls to what you would see at your bank"*
   ** "robust authentication, including two-factor verification"*
   ** "Its data security and privacy requirements have been assessed against government standards for the use of cloud-hosted services."*

   When the NZ Police Firearms Safety Authority sends a letter to a firearms licence holder it uses encrypted PDFs documents to keep information "secure". I am deliberately not providing details of this to help protect the use of security through obscurity.

   Can the NZ Police confirm that the security of all communications align with the security requirements and guideance provided by the NZ Government Communications Security Bureau, especially, but not limted to, the following sections:
   ** 16.1.15*
   ** 16.1.19*
   ** 16.1.20*
   ** 16.1.21*

This part of your request has been interpreted as being about the Arms Information System (AIS) which houses the Firearms Registry. The AIS holds no passwords. AIS authentication is provided by the Department of Internal Affairs (DIA) via RealMe for public users, and enforces two-factor authentication either by SMS or authenticator app.

For internal Police access which include Te Tari Pūreke – Firearms Safety Authority, access is restricted to the Police network, and password complexity and storage is controlled by the Police enterprise password policies which conform to the New Zealand Information Security Manual (NZISM) standards.

However, the following sections relate to RealMe security, therefore Te Tari Pūreke has transferred this part of your request to DIA as the information is believed to be more closely related to their functions. Please expect a response from DIA in due course.

** 16.1.40.R.03*
** 16.1.40.R.04*
** 16.1.40.C.02*
** 16.1.41.R.01*

Te Tari Pūreke certification and accreditation confirms what the systems are evaluated against and that they comply with NZISM standards.

Please refer to the NZISM Certification and Accreditation standards below, which is publicly available through the following website link https://nzism.gcsb.govt.nz/ism-document/pdf/Section/12460:

> 4.1.11. Certification is the assertion that an ICT system including any related or support services such as Telecommunications or cloud comply with the minimum

standards and controls described in the NZISM, any relevant legislation and regulation and other relevant standards. It is based on a comprehensive evaluation or systems audit

4.1.12. Certification is evidence that due consideration has been paid to risk, security, functionality, business requirements and is a fundamental part of information systems governance and assurance

4.1.16. Accreditation is the formal authority to operate a system, evidence that governance requirements have been addressed and that the Chief Executive has fulfilled the requirement to manage risk on behalf of the organisation and stakeholders. This element of the C&A process is described in Section 4.4 – Accreditation Framework

4.1.17. Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged, including the acceptance of any residual risk.

In addition, please find attached the following documents:

- Letter of Security Certification - Arms Information System using Objective RegWorks (December 2023)
- Certificate of Accreditation NZPOL-202312-FIREARMS-AIS
- Simply Privacy – Independent Privacy Impact Assessment on the AIS Registry and Service Centre.

Note that some information within these documents have been withheld under the following sections of the OIA:

- 6(c): where release would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial
- 9(2)(a): to protect the privacy of natural persons
- 9(2)(k): to prevent the disclosure or use of official information for improper gain or improper advantage.

Police considers the interests requiring protection by withholding the information are not outweighed by any public interest in release of the information.

You have the right to ask the Ombudsman to review this decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz.

For your information, Police has developed a process for proactive release of information, so the anonymised response to your request may be publicly released on the New Zealand Police website.

Nāku noa, nā

Matthew Boddy
Acting Director Operations
Firearms Safety Authority

Letter of Security Certification

System	**Arms Information System (AIS) based on Objective RegWorks**
To Accreditation Authority	Mike Webb (Chief Assurance Officer)
From Certification Authority	Jay Garden (Chief Information Security Officer)
Date	25 November 2022, and 13 June 2023. Updated 19 December 2023

Purpose

Accreditation of the Arms Information System (AIS) based on Objective RegWorks cloud services has been requested by the business owner, Angela Brazier, Executive Director Firearms, Te Tari Pūreke. This letter of security certification, along with the attached supporting documentation, is in support of an Accreditation decision from the Police Accreditation Authority.

The AIS system – including the R2 registry public interfaces and integrations – was provided Qualified Accreditation in June 2023.

System and Project Background

AIS is a new firearms registry and associated online services as part of the Arms Transformation Programme and firearms control reform managed by Te Tari Pūreke.

AIS is based on one of Objective's cloud Software as a Service offerings, RegWorks, which is designed to support regulation, compliance and enforcement (https://nz.objective.com/products/objective-regworks).

Objective uses Amazon Web Services (AWS) Infrastructure as a Service to host the RegWorks services. A private/single tenant instance of the RegWorks platform specifically for AIS has been established on the Australian AWS platform and data centres.

AIS's first iteration (Release 1), being certified in this report, does not provide the registry functionality, which is planned for next year. It does provide the initial set of forms for public interaction with the NZ Police firearms teams; replacing functionality that had been provided by PEGA Firearms and the 105 Forms services:

- Online forms portal, with authentication using RealMe
- Online forms back office, with authentication using Azure AD
- Outbound email
- Card payments using Spreedly and Paystation
- Address validation via Google
- NZBN validation via MBIE

The users of AIS are the public (e.g. to renew a firearms license), Regulator staff within NZ Police, and partner staff such as MFAT and Customs.

The bulk of the information handled by AIS will be IN CONFIDENCE, but it is likely to handle some SENSITIVE information (e.g. information on restricted firearms and the owners that could put those people at risk if the information was discovered by criminals). The registry as a whole is treated as RESTRICTED due to the effect a breach would have in the public's trust and confidence in NZ Police.

The key changes for R2 were:

- Establishes a *Registry of Firearms*
- Bidirectional (read-only) integration with NIA for licensing and registry information

- MyFirearms portal for the public, e.g. firearms owners and dealers
- Dealer Transactions via a form on the 105 website s.9(2)(k) OIA
- Expanded internal user base for AIS
- Registry information will be replicated into the Data Warehouse for SAS/BO/PowerBI consumption.

Assurance

Objective RegWorks has ISO27001 and Australian IRAP certification. It is a GCDO-approved cloud service for IN CONFIDENCE information, and it is already in use by various New Zealand and Australian government agencies.

Assurance over the risk and security processes for the AIS instance has been conducted Michael O'Connor of Lateral Security. The High Assurance certification process has been used.

Penetration testing of the *application* was conducted by ZX Security, with some deficiencies noted. The *platform* security was reviewed s.9(2)(k) OIA

Residual Risk

The security risk assessment process assessed the overall level of inherent risk of AIS to be HIGH. With all existing and planned controls in place, the expected and current risk is assessed as MEDIUM (13: Unlikely chance of Major damage).

Most controls are now in place and have been assessed as being effective, but some are incomplete, or we have not been able to gain assurance over, particularly relating to:

- s.9(2)(k) OIA

The business owner, Angela Brazier, Executive Director Firearms, has endorsed the risk assessment and associated security controls.

s.9(2)(k) OIA

- **Governance and project controls**: All parties involved with management and development of AIS understand their responsibilities. A PIA and a GCDO105 questionnaire have been completed. RegWorks has Payment Card security standard (PCI-DSS) certification but compliance of the AIS instance has not yet been verified.

- **System design and implementation**: RegWorks is a relatively mature product and appears to be largely fit for purpose. Mechanisms such as MFA/two-step authentication, encryption and data back-up services are used as expected. Detailed design documentation has not been provided to NZ Police, which is not uncommon for a SaaS product, s.9(2)(k) OIA [redacted]
- **Physical and personnel security**: The security of the data centres and servers are suitable, as are the controls around Objective's own facilities for the activities that they will perform. All activities are based in Australasia.
- **Operational controls**: s.9(2)(k) OIA [redacted] but in general the Objective-AWS service management processes appear adequate. Finalising the AIS service management specifics and integration into the NZ Police ICT and business processes is still in progress.

In summary, I believe that the controls and assurance are adequate for the current AIS functionality and phase of the firearms programme.

A lot of good work has been done to help secure the AIS platform and provide increased assurance that the controls are effective, but a range of key security and management controls are still a work-in-progress. The security risks have decreased but it will be important to continue to improve both the technical solution and integrated service management practices across ASW, Objective, Te Tari Pūreke and the NZP Cyber Security Operations Centre).

Accreditation Recommendation

I have examined the RegWorks AIS risks, controls and security evidence provided by the project and the assurance process.

There is still some work to be completed to ensure all security risks will be managed effectively and confidently, but the system and its management processes are now at a point that I can recommend it to be awarded **Full Accreditation** for **three years.**

Certificate of Accreditation

This is to certify that the

Firearms Regulator Arms Information System (AIS)

using

Objective RegWorks

has been awarded **Full Accreditation** for **three years** until

20 December 2026

Signed: s.9(2)(a) OIA

Date: 20 December 2023

Certificate No: NZPOL-202312-FIREARMS-AIS

Chief Assurance officer

De-facto Accreditation Authority

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

Simply Privacy

New Zealand Police
Ngā Pirimihana o Aotearoa

Privacy Impact Assessment on the AIS Registry and Service Centre

Version 1.0
28 April 2023

Contents

Executive summary **4**
Glossary of terms **7**
1. About this PIA **8**
1.1 Purpose and scope 8
1.2 The information we have considered 9
1.3 How we structure the PIA 9
1.4 About us 10
2. Context **11**
2.1 Privacy Act mandates a risk-based approach 11
2.2 IPPs provide a reasonable set of rules 11
2.3 DPUP complements these rules 12
2.4 Māori privacy perspectives are relevant 13
2.5 Firearms community is sensitive about privacy 13
2.6 The overall privacy risk profile is high 14
2.7 Relationship between Te Tari Pūreke and Police 14
3. Project **16**
3.1 Background 16
3.2 Legislative Framework for the Registry 16
3.3 Key components of the AIS 17
4. Personal information **19**
4.1 Personal information involved 19
4.2 High-level data flows 20
5. Summary of IPP application **24**
6. Privacy risk and opportunity assessment **28**
6.1 Managing service provider risk 28
6.2 Governance of the Registry and its data 31
6.3 Security as foundation of trust 33
6.4 Managing work from home risk 33
6.5 Enabling safe public access to data 36
6.6 Privacy training for Te Tari Pūreke 41
6.7 Privacy transparency 42
6.8 Safely leveraging Registry data 43
6.9 Risk-assessing new technological features 44
6.10 Other compliance issues 45
Appendix 1: Information gathering **48**
Appendix 2: Recommendations action plan **49**

Version	Date	Author	Comments
0.1	27 March 2023	Daimhin Warner Emma Pond	First draft for consultation
0.2	3 April 2023	Daimhin Warner Emma Pond	Incorporating initial feedback from project team and privacy team
0.3	4 April 2023	Daimhin Warner	Minor additional amendment requested by project team
1.0	28 April 2023	Daimhin Warner	Final version, including minor final additions

Executive summary

This is an independent Privacy Impact Assessment (**PIA**) of the privacy risks involved with establishing a new capability for the registration of firearms, the Firearms Registry (**Registry**) which will sit within the Arms Information System (**AIS**). The Registry is being delivered for Te Tari Pūreke as part of the Arms Transformation Programme, a programme of work to reform New Zealand's arms system.

This PIA is intended to provide assurance to Police in respect of the design and implementation of the Registry, the Service Centre, and their associated processes. However, it is also intended to assist Te Tari Pūreke to build trust with the firearms community, by demonstrating the importance Te Tari Pūreke has placed on ensuring that privacy and security have been robustly considered and addressed.

There are three key factors that significantly raise the privacy risk profile for the AIS. The first is the inherent sensitivity of the personal information being collected and processed for the purposes of the Registry. The second is the real potential for harm (to the individuals concerned and the community) if this information is subject to a privacy breach. The third is the high level of sensitivity displayed by the firearms community in relation to the development and operation of the Registry. For these reasons, a failure to protect Registry data could have a major negative impact on Te Tari Pūreke and could derail legitimate efforts to better regulate the use of firearms in New Zealand.

On this basis, it will be critical for Police to ensure that security and privacy controls – including those recommended in this PIA – are in place on Day 1. Security and privacy must be viewed as a core requirement before launch, not an eventual add-on. Teething problems will inevitably arise as the Registry is launched, particularly because new staff will be using new systems and exercising newly gained knowledge. This is when human error is most likely to occur. Ensuring that technical and organisational security and privacy controls have already been implemented will mitigate this risk. This will also protect the Registry and its data at a time when the system will be under significant scrutiny from the firearms community.

The DPUP principles of Kaitiakitanga and Mana Whakahaere are highly relevant to the AIS project. Te Tari Pūreke will need to ensure that it acts as a steward of firearms information in a way that the firearms community understands and trusts. It will also need to take steps to empower the firearms community through transparency, access, and oversight. The observations and recommendations made in this PIA will assist Te Tari Pūreke to meet these important principles, and ensure that from Day 1 onwards, Te Tari Pūreke can deliver on its legislative mandate while protecting the privacy of the firearms community.

Recommendation	Page
Rec-001: Assign Data Owners for the personal information Te Tari Pūreke holds, to reduce the risk of scope creep.	31

Recommendation	Page
Rec-002: Establish and communicate clear escalation rules for Te Tari Pūreke privacy and security risks and events.	31
Rec-003: Consider how best to ensure Te Tari Pūreke receives the ongoing privacy expert support it needs to manage its specific privacy risk profile and ensure the protection of the sensitive personal information it holds.	31
s.9(2)(k) OIA [redacted]	32
Rec-005: Where appropriate and practicable, implement a similar approach for AIS monitoring and audit as is currently applied to the NIA.	32
s.9(2)(k) OIA [redacted]	33
s.9(2)(k) OIA [redacted]	33
	34
	35
	36
Rec-011: Consider developing a process to flag and manage a known risk to a firearms licence holder's account, on the basis of possible impersonation attempts.	39
Rec-012: Consider developing guidance for Registry Service Centre staff to identify and manage difficult request scenarios, including requests from representatives.	39
Rec-013: Support Registry Service Centre staff to take a robust approach to managing the identity verification process, including by avoiding performance measures linked solely to numbers of callers verified or customer experience scores.	39

Recommendation	Page
Rec-014: Engage with the dealer community to explain the risks associated with releasing dealer reports, and to fully understand the needs of dealer licence holders, before finalising the possible controls to manage the privacy risk associated with this process.	41
Rec-015: Ensure routine customer service communications to firearms licence holders contain the minimum personal information possible to achieve their goal.	41
Rec-016: Develop and deliver Te Tari Pūreke-specific privacy and security training to all staff prior to Day 1.	42
Rec-017: Develop a standalone privacy statement for the Registry, aimed at providing assurances to the firearms community that Registry data will be managed with care and used only for a limited set of legitimate regulatory and law enforcement purposes.	43
Rec-018: Put controls in place to mitigate risks associated with using Registry and dealer transaction data for broader analytics purposes.	44
s.9(2)(k) OIA [redacted]	45
s.9(2)(k) OIA [redacted]	46
Rec-021: Develop data retention rules for non-Registry information held by Te Tari Pūreke that align to Police's general practice, and ensure Te Tari Pūreke systems are configured to comply with these retention rules.	47

Glossary of terms

Term	Definition
AIS	Arms Information System – The entire system developed for the purposes of managing the Registry, including the MyFirearms online portal and the Registry itself, hosted on RegWorks by Objective.
Constabulary	The part of the Police responsible for managing the Police's law enforcement functions. The term is used to distinguish this part from the Regulator (Te Tari Pūreke).
IPPs	Information Privacy Principles, contained in section 22 of the Privacy Act 2020.
NIA	National Intelligence Application – Police's central system for managing law enforcement information, including personal information.
Personal information	Any information about an identifiable individual, including information about firearms licence holders and dealer licence holders, but not including information about incorporated entities (such as gun shops or shooting clubs).
PIA	Privacy Impact Assessment, a risk assessment used to help agencies identify and evaluate the potential privacy impact of a project, process, or change.
Regulated party	Any party required by the Arms Act 1983 and associated regulations to provide information to the Registry. Regulated parties include firearms licence holders, dealer licence holders and shooting clubs.
Regulator	The agency established to administer the Arms Act 1983 and maintain the Registry. The Regulator is the Te Tari Pūreke - Firearms Safety Authority.
Te Tari Pūreke	Firearms Safety Authority – the Regulator established to administer the Arms Act 1983. Te Tari Pūreke is a part of NZ Police.

1. About this PIA

A Privacy Impact Assessment (**PIA**) is an essential part of the project lifecycle, used to help agencies identify and evaluate the potential privacy impact of a project, process or change. A PIA can give an agency a better understanding of information flows, help it to make more informed decisions, better manage privacy risks, and promote a positive sum outcome that delivers the desired benefits in a way that protects individual privacy.

1.1 Purpose and scope

This is an independent PIA of the privacy risks involved with establishing a new capability for the registration of firearms, the Firearms Registry (**Registry**) which will sit within the Arms Information System (**AIS**). The Registry is being delivered for Te Tari Pūreke as part of the Arms Transformation Programme, a programme of work to reform New Zealand's arms system. The PIA assesses and identifies privacy risks in relation to the Registry and Service Centre (call centre) that will support it. Where possible, recommendations are made to enable Te Tari Pūreke to address those risks.

This PIA is intended to provide assurance to Te Tari Pūreke in respect of the design and implementation of the Registry, the Service Centre, and their associated processes. However, it is also intended to assist Te Tari Pūreke to build trust with the firearms community, by demonstrating the importance it has placed on ensuring that privacy and security have been robustly considered and addressed.

In scope	Out of scope
• Privacy implications of the developments to be delivered as part of Release 2.1, relating to the development of the Registry and Service Centre and their associated processes. • Privacy implications of using several third-party service providers to deliver components of the Registry and Service Centre, including in relation to data control and jurisdictional risk. • High-level consideration of managing data analytics and reporting processes in a privacy compliant manner.	• Technical security risks created by the Registry and Service Centre. While security is an important element of the privacy framework, and this PIA may identify high-level security risks, this is not a security assessment. • Privacy risks created by existing processes that feed into the AIS, such as the firearms licensing process, other than where this is directly relevant to the Registry or Service Centre. • MyFirearms portal usage data (including data generated by cookies), which is already implemented, and not changing as part of Release 2.1. • Functions or processes to be implemented in future releases, such as those being

In scope	Out of scope
	delivered in Release 2.2 (with the exception of the data analytics issue noted to the left).

1.2 The information we have considered

We interviewed key project stakeholders and subject matter experts, with a view to understanding the policy and legislative context for the AIS, the detailed proposed requirements and design of the Registry and Service Centre, and the data flows that underpin them. We also reviewed key project documentation, including cabinet papers, discussion documents, summary of public submissions, business cases, contracts, high-level and detailed requirement documents, existing policies and procedures, and privacy and security risk assessments already completed by the Police. A full list of stakeholders interviewed, and documents reviewed is set out in Appendix 1.

1.3 How we structure the PIA

The PIA is in five sections, covering contextual considerations, an overview of the project, application of the information privacy principles (**IPPs**) and a more in-depth privacy risk and opportunity assessment. Throughout the PIA, recommendations are highlighted in yellow, and key observations are highlighted in blue. The recommendations are prioritised in Appendix 2.

Context	This section will outline the relevant regulatory and other contexts within which this PIA is completed, including the Privacy Act and Data Protection and Use Policy, and public concerns about firearms information.
Project	This section will outline Simply Privacy's understanding of the Registry and Service Centre, from a technical, operational, contractual and governance perspective.
Personal information	This section will outline the data flows required to manage the Registry and Service Centre and the services they enable.
Summary of IPP application	This section will summarise the application of the IPPs to the Registry and Service Centre, with a view to identifying areas of risk and opportunity that should be given more detailed consideration.
Privacy risk and opportunity assessment	This section will assess in more depth the key privacy risks and opportunities identified in relation to the Registry and Service Centre. Here, we will also provide recommended solutions and mitigations to risks, where possible.

1.4 About us

Simply Privacy is one of NZ's leading privacy consultancies. We provide privacy strategy, risk analysis, and consultancy services to public and private sector agencies in NZ and around the world. Simply Privacy's principals are experts in the field, having previously held senior roles with the Office of the Privacy Commissioner, and senior in-house privacy roles. Simply Privacy has provided strategic, maturity, risk assessment, advisory and other privacy services to numerous government agencies.

In preparing this assessment, Simply Privacy has relied upon information, statements and representations provided to it by Police. Simply Privacy provides no warranty of completeness, accuracy, or reliability in relation to this information, these statements, or these representations.

This assessment is not legal advice, and its contents should not be taken as legal advice.

2. Context

2.1 Privacy Act mandates a risk-based approach

This PIA takes a risk-based approach, consistent with general principles of Privacy by Design. It does not look for outcomes that protect privacy at the total expense of other risks. Rather, it recognises that privacy is one of many risks Police must address. The Privacy Act itself facilitates this approach, providing that the right to privacy may be balanced against other important rights and interests, including the general desirability of a free flow of information and the right of business and government to achieve their objectives efficiently.

The Privacy Act is a "how to", not a "do not do"

In a recent submission to the High Court relating to access to Ministry of Health Covid-19 data by a Māori health service provider,[1] the Privacy Commissioner described the Privacy Act as a "how to", not a "do not do". They were referring to the fact that the Privacy Act is a flexible, principles-based law that is intended to enable organisations to meet their legitimate purposes.

This means privacy risk must not be viewed in isolation. When assessing privacy risks and opportunities in relation to the AIS, we must consider the Police's other legal and contractual obligations, their ability to deliver services efficiently and effectively, and the broader community benefits of properly managing firearms risk.

2.2 IPPs provide a reasonable set of rules

The Privacy Act 2020 contains 13 information privacy principles (**IPPs**), summarised in section 5, which provide agencies with a roadmap for managing personal information, from collection through to destruction. They are mandatory, but flexible enough to permit agencies to collect, use and share the information they need to perform their lawful functions. Many of the IPPs contain exceptions that ensure privacy does not become a barrier to legitimate, lawful and proportionate government or business outcomes.

The Act anticipates a pragmatic interpretation of the IPPs. The exceptions to the IPPs generally incorporate an element of reasonableness. Further, application of the IPPs is subject to any other law that specifically authorises or requires personal information to be made available, restricts the availability of personal information, regulates the manner in which personal information may be made available, or authorises any action in relation to personal information. This includes the Arms Act and associated regulations.

[1] https://www.courtsofnz.govt.nz/assets/cases/2021/2021-NZHC-3319.pdf.

2.3 DPUP complements these rules

The government has developed a Data Protection and Use Policy (**DPUP**), aimed at assisting public sector agencies to build strong relationships with individuals and communities. It does this through a set of DPUP principles relating to the respectful, trustworthy, and transparent collection and use of information about people, whānau and communities.

He Tāngata - Focus on improving people's lives — individuals, children and young people, whānau, iwi and communities. This incorporates privacy concepts such as data minimisation, purpose specification, and the creation of positive outcomes from data use.

Manaakitanga - Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information. This incorporates recognition of diverse cultural perspectives about data, and requires meaningful partnership with affected service users.

Mana Whakahaere - Empower people by giving them choice and enabling their access to, and use of, their data and information. This incorporates privacy concepts such as meaningful transparency, consent, and subject access and correction rights.

Kaitiakitanga - Act as a steward in a way people understand and trust. This incorporates privacy concepts such as data protection (security), accountability, and privacy breach notification.

Mahitahitanga - Work as equals to create and share valuable knowledge. This incorporates sharing data in ways that decrease the burden on service users and ensure the best outcomes for people and their communities, and also ensuring that de-identified data can be used for research and evaluation (though note specific open data risks discussed below).

Though not mandatory, agencies are encouraged to adopt DPUP in a way that makes sense for their work and their communities. In addition, each year the Government Chief Privacy Officer asks public sector agencies to submit a self-assessed Privacy Maturity Assessment which is based on the DPUP.

The principles of **Kaitiakitanga** and **Mana Whakahaere** have particular relevance to the AIS project. Te Tari Pūreke will need to ensure that it acts as a steward of firearms information in a way that the firearms community understands and trusts. It will also need to take steps to empower the firearms community through transparency, access, and oversight.

Where a section of the PIA has direct relevance to one of the DPUP principles above, this is indicated with the relevant icon. For example, sections on information security and governance will support Te Tari Pūreke to comply with the principle of Kaitiakitanga.

2.4 Māori privacy perspectives are relevant

Te Tari Pūreke will need to ensure that it develops and implements the Registry and Service Centre in a way that complies with its obligations under the Treaty of Waitangi, including consideration of the Treaty principles of partnership, participation and protection.

The AIS, and the services it enables, will involve the processing of personal information about Māori individuals and communities. We understand that Te Tari Pūreke has undertaken some engagement in this area in respect of the ATP and specifically the AIS, and we recommend it continue to do so.

We also note the Privacy Act 2020 requires the Privacy Commisioner to take cultural perspectives on privacy into account when performing their duties, as does the DPUP principle of **Manaakitanga**.

2.5 Firearms community is sensitive about privacy

Te Tari Pūreke will need to be mindful of the context within which the Registry is being developed. The general sensitivity of information about the possession (and location) of firearms, coupled with several unfortunate incidents relating to how such information has been handled, have created a high level of sensitivity among the firearms community around privacy and security. This context increases the privacy risk profile for the Registry, and will need to influence risk-based decisions relating to privacy and security.

Recent high-profile breaches involving personal information about firearms licence holders include the following:

- In 2019, information about more than 37,000 firearms owners – including the firearms they possessed and financial information – collected as part of the firearms buyback scheme was inadvertently made accessible to a group of dealers as a result of a software update by the developer SAP. The breach prompted some to call into question the intention to create a firearms registry.[2]

- In 2021, a Police email error resulted in the disclosure of email addresses for nearly 40 firearms owners. An email, advising firearms owners to take a firearms safety course, was sent without using the blind copy function, which meant recipients could view the email addresses of other firearms owners. While this was not a significant privacy breach, it reignited public concern with and criticism of the planned firearms registry.[3]

- In 2022, firearms licencing documents were stolen from the former Auckland Central Police Station, and located among stolen property during a Police operation. The

[2] 2019 breach involving the gun buy-back registry.
[3] 2021 breach involving email error.

information included the names and addresses of firearms licence holders. As a result, the Police urged firearms owners to secure their firearms. Relevant to this PIA, the Privacy Commissioner commented in relation to the breach that the Police needed to take "a whole-of-life approach to safeguarding information, including carefully disposing of it once it is no longer required to avoid the risk of it being inadvertently shared".[4]

The recent consultation process on the drafting of Arms Act regulations for the Registry indicates that the firearms community has been affected by these breaches, and that it has concerns about the Police's ability to safeguard Registry information. The following is a summary of privacy concerns raised in submissions on the August 2022 discussion document:

- There is a lack of confidence in the Police's ability to keep Registry information safe, secure and accurate.
- The Registry could be vulnerable to hacking, and information could fall into the hands of criminals.
- Personal details (such as names and addresses) should be stored separately to firearms details, to reduce risk in the event of a privacy breach.
- It is too risky to have a data repository of firearms and ammunition storage locations. This could become a "shopping list" for criminals.
- Too many people may have access to the Registry, and the wider the access, the higher the risk of misuse.
- The retention period for Registry data is too long, and retaining it after the death of a licence holder could cause a security risk to their family.

2.6 The overall privacy risk profile is high

There are three key factors that significantly raise the privacy risk profile for the AIS. The first is the inherent sensitivity of the personal information being collected and processed for the purposes of the Registry. The second is the real potential for harm (to the individuals concerned and the community) if this information is subject to a privacy breach. The third is the high level of sensitivity displayed by the firearms community in relation to the development and operation of the Registry. For these reasons, a failure to protect Registry data could have a major negative impact on Te Tari Pūreke and could derail legitimate efforts to better regulate the use of firearms in New Zealand. The findings and recommendations made in the PIA reflect this.

2.7 Relationship between Te Tari Pūreke and Police

Te Tari Pūreke is a functional unit within the Police. This means that, for the purposes of the Privacy Act, the Police is the "agency" that is holds Te Tari Pūreke data. However, because Te

[4] 2022 breach involving theft of documents from Vincent St station.

Tari Pūreke – as a regulator – has a distinct legislative mandate to administer the Arms Act, and in view of the high privacy risk profile identified above at section 2.6, it will be important to maintain an appropriate level of functional separation between Te Tari Pūreke and the Constabulary. While the sharing of information between the two functions is not a "disclosure" for the purposes of IPP 11 of the Privacy Act, access to Registry information by the Constabulary (or any other functional unit within the Police) should be carefully managed to reduce privacy and security risk and maintain the trust and confidence of the firearms community. Several of the observations and recommendations made in this PIA are intended to support this functional separation where appropriate.

3. Project

3.1 Background

In 2020, several changes were made to the Arms Act 1983 through the Arms Legislation Act 2020, to strengthen the control and regulation of firearms in Aotearoa. The changes reflect the Act's principles that possessing a firearm is a privilege, and people with that privilege have a responsibility to act in the interests of personal and public safety. Not all the changes have come into force at the same time. Instead, implementation is in phases. The next group of changes will come into force on 24 June 2023 (**Day 1**).

These changes provide for the establishment of a Registry to store and link information on all firearms and other arms items and their licence holders. This will enable greater and more centralised oversight of the number and location of firearms and other arms items in New Zealand.

Police already holds information on all licence holders and any prohibited firearms, prohibited magazines, pistols and restricted weapons they may have. The latter information is collected through the endorsement requirements combined with the application and notification process for permits to possess or import.

All firearms and other specified items need import permits. Police receives notifications from licence holders when they receive these imported items. However, if standard (non-prohibited) firearms are on-sold or otherwise transferred after import, there is currently no way of knowing who has transferred them and to whom or how securely they are held. This makes it easy for people with criminal intentions to get around the regulations through unrecorded changes of possession. To discourage this, the Registry will store information on all regulated arms items held, obtained, and transferred by all licence holders, as well as other information to be specified in regulations.

From Day 1, the Act will prescribe the staged gathering of information by the Registry on arms items possessed by licence holders at that date. It requires licensed persons and any other persons specified in regulations to provide up to date information for the registry on all items in their possession at the time when specified circumstances take place during the first five years of the Registry. Specified circumstances include when applying for a licence or endorsement, changing address, or buying or selling arms or ammunition.

3.2 Legislative Framework for the Registry

New provisions on the Registry, which come into force on 24 June 2023, can be found in the Arms Legislation Act 2020 in:

- Section 104, which inserts new sections 93 to 95 into the Arms Act. These sections cover the establishment of the Registry, the content of the Registry and obligations to provide information to the Registry.
- Section 63, which inserts new sections 38Y to 38ZH in Part 7 into the Act which cover direct access by specified government agencies to the Registry.
- Section 84, which inserts section 58A into the Act which sets out offences relating to the Registry.
- Section 105, which inserts new clause 14 of Schedule 1 into the Act. This clause sets out transitional provisions that apply after 24 June 2023 for obtaining information for the Registry.

There are provisions in the Act that enable the making of regulations to help implement the Registry (section 74(1) (pa) and (pc)). In October 2022, the Police engaged in a public consultation on the content of these regulations, seeking submissions on a discussion document that set out the proposed data elements that would be required for the Registry, the events that would trigger a requirement to register a firearm, and timeframes for the registration of firearms.

This discission paper prompted a significant amount of concern and interest from submitters. The key submissions as relevant to this PIA are set out above at section 2.5. The submissions resulted in some changes to the proposed regulations, with the final objectives for the regulations set out in a Cabinet Paper and reflected where relevant in this PIA.

3.3 Key components of the AIS

Te Tari Pūreke's vision is to become a "**modern, technology-enabled regulator that can apply its people and resources effectively to support licence holders in meeting their obligations**". The development of the AIS and its various components and supporting processes, are intended to enable this vision, making it easier for both the Regulator and regulated parties to meet their obligations.

3.3.1 MyFirearms portal

The MyFirearms portal was developed to enable Police to better manage the firearms licensing process. Operational since late 2022, it moves the previous paper-based processes online, including applying for or renewing firearms licences. It provides firearms licence holders and/or applicants with the ability to create an account (using RealMe), apply for or renew a licence or endorsement, update their personal details, and pay any fees online.

From Day 1, MyFirearms will also provide those firearms licence holders who are registered users with functionality to register their arms items online. Other functionality (such as the ability to view details of their licence, contact details, and registered arms items) will only be available to MyFirearms users who have had their identity validated via an in-person process

(either as part of a new licence holder application or via a separate in personal validation process).

The MyFirearms portal interfaces with the AIS. The AIS is hosted on a third-party SaaS platform called Regworks, provided by Objective.

3.3.2 Registry

The Registry itself will sit within the AIS, and will be populated by data provided by regulated parties or pulled from NIA. The AIS will integrate with NIA in order to automatically link the MyFirearms account/user to the corresponding NIA licence holder record. There will also be a data flow from the Registry back to NIA of the details of firearms held by that licence holder once those firearms are registered. In addition, the Registry will integrate with a data warehouse for reporting purposes.

Te Tari Pūreke staff will access the Registry to carry out administrative and compliance functions associated with the registration of firearms. These activities will include managing aspects of firearms registration such as transfers, record modifications and amendments, and updating export records.

3.3.3 Service Centre

To ensure that Te Tari Pūreke and regulated parties can be compliant with their obligations under the Arms Act and the new regulations, initial digital capability for Day 1 will be supplemented with a mix of digital and non-digital channels.

The Service Centre will be the interface for individuals who do not have access to, or are not confident using, the MyFirearms channel. Up to 80 agents (Administrators and Officers) will be available to support licence holders complete the digital forms on their behalf and answer any queries about the Arms Act and its obligations. In addition, the Service Centre will help regulated parties to meet their obligations in respect of transferring firearms, as this functionality will not be available digitally via MyFirearms on Day 1. The Service Centre will also support other users of the Registry such as dealer licence holders.

The Service Centre will use the Genesys cloud TaaS platform to provide this service (discussed further below), including call recording, chatbot and possible transcription functionality.

4. Personal information

4.1 Personal information involved

Te Tari Pūreke needs to collect and process a significant amount of personal information about regulated parties, for the broad purpose of supporting Te Tari Pūreke to deliver to its legislative mandate.

The Arms Act states that the following information **must** be recorded in the Registry:

- Information about the (firearms or dealer) licence holder:
  - full name
  - date of birth
  - residential address
- Information about each of the licence holder's licences:
  - licence number
  - expiry date
  - endorsements and conditions
- Every arms item possessed by the licence holder, and the location of that arms item (with particulars specified in regulations)[5]
- Whether the licence holder is an ammunition seller
- Any information required by regulations to be recorded (see below).

The Arms Act states that the following information **may** be recorded in the Registry:

- Photographs of applicants
- Any other information considered desirable by the Commissioner.

It is proposed that the Regulations for the Firearms Registry will require every regulated party to provide the following for inclusion in the Registry (some of which may be pre-populated by Police if it is already held in NIA):

Firearms licence holder	Dealer's licence holder
• Email address • Phone number • Postal address (if different from residential address) • Information about approved storage locations.	• Email address(es) • Phone number(s) • Registered name of business, trading name, and NZBN • Business address(es) • Postal address(es) • Storage facility address(es) • Names and firearms license numbers of dealer employees.

[5] Note, registration of dealer licence holder arms items will not be included in release 2.1, and is not in scope for this PIA.

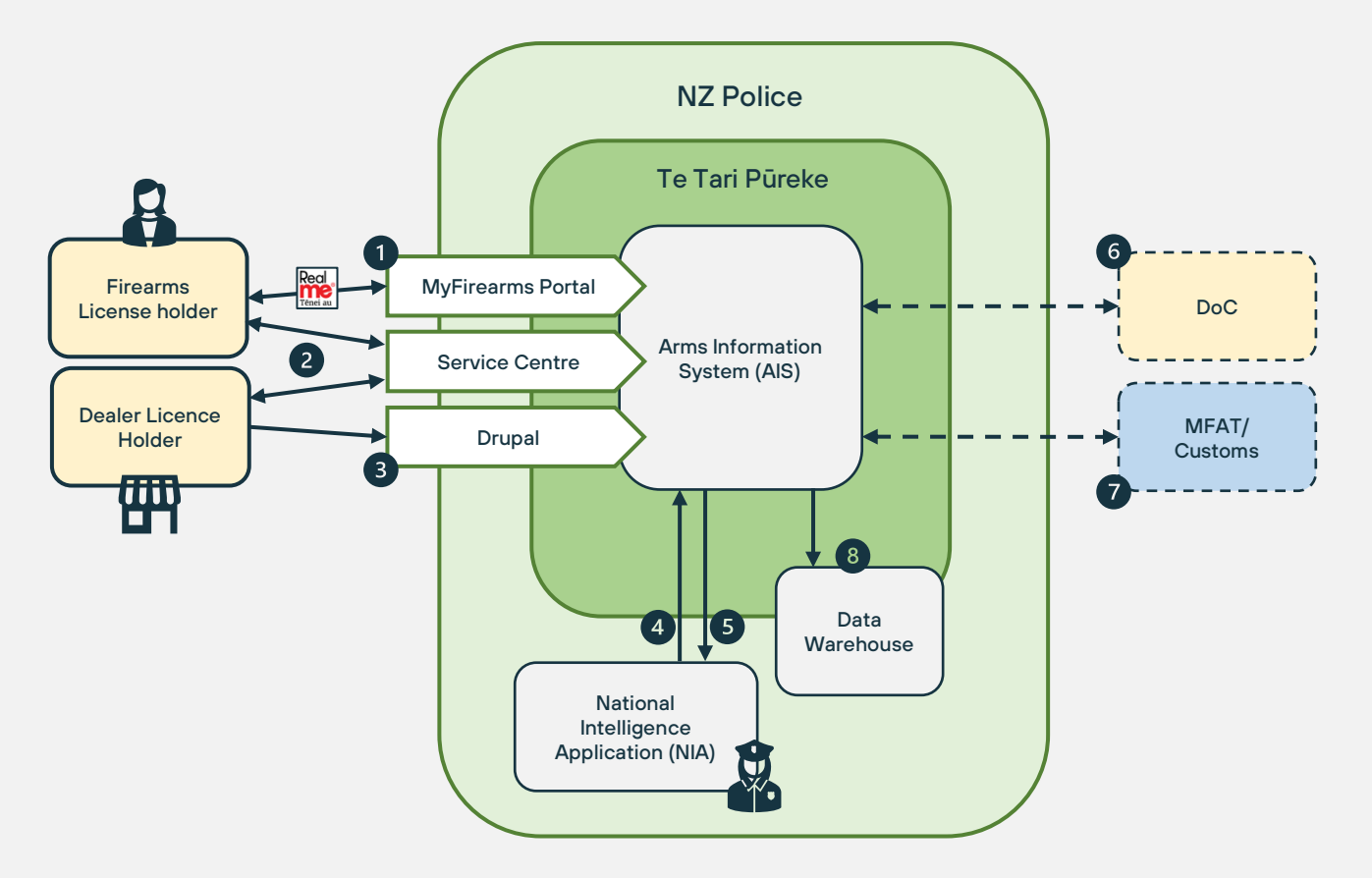
The Regulations for the Firearms Registry will also specify the particulars of each arms item that will need to be recorded in the Registry (such as make, model, type, calibre etc). These particulars are not especially relevant to this PIA, for the purposes of which it is enough simply to note that the Registry will associate arms items (and their particulars) to a licence holder.

Te Tari Pūreke will also collect the following information that is not required by the Arms Act or regulations, but is required for legitimate business purposes related to managing the Registry and associated processes:

- MyFirearms portal usage data, such as device location, page clicks, and activities once logged in
- Call recordings of all calls to and from Service Centre
- Files notes of enquiry calls that require a call back
- Chat enquiry records (which may contain identifiable information)
- Emails to and from regulated parties and enquirers.

4.2 High-level data flows

Figure 1 – High-level data flows



1. A firearms licence holder will register with MyFirearms and create an account. To do this, they must sign in with their RealMe account and link their MyFirearms account to their RealMe identity. Note that at this stage the RealMe account does not have to be verified. Once an account is locked (and the identity has been matched with an existing firearms licence holder), the firearms licence holder can perform a restricted range of "safe actions", including registering arms items against their licence. However, they cannot view all arms items registered to that licence(s), historical submissions, or licence details.

   In order to perform all available activities on MyFirearms, the firearms licence holder must "validate" their account against their firearms licence. This requires an in-person validation against the verified identity data held in the AIS and the licence data held in the NIA. This allows for Te Tari Pūreke to ensure that the correct individual is matched with the correct firearms licence.

   Once validated, a firearms licence holder can view all the data associated with their licence(s), including all arms items registered (whether online or by back office) and other relevant submissions. They can draft and edit submissions made to the Registry within the portal, and can "maintain arms item details", thereby ensuring the Registry is accurate and up to date. A firearms licence holder cannot make changes to their licence holder details – this must be completed via the Service Centre.

   Te Tari Pūreke will communicate with a firearms licence holder about their online submissions, including sending email acknowledgements and updates in relation to submissions, and email alerts where a trigger event (such as an arms item transfer) requires the firearms licence holder to update the Registry (for example by registering a new arms item they have purchased).

2. All regulated parties can use the Registry Service Centre to interact with Te Tari Pūreke and the Registry. This might occur where the regulated party has no access to the Internet or prefers not to use the MyFirearms portal. A regulated party may register an arms item, notify Te Tari Pūreke of an arms item transfer, notify Te Tari Pūreke of the loss, theft or destruction of a registered arms item, or request to change details via the Service Centre. The Service Centre employee will then make the required changes to the AIS.

   The Service Centre will also manage general enquiries about the Registry, which may come from firearms licence holders, dealer licence holders, or members of the public. The Service Centre will also manage email correspondence with regulated parties or enquiries and the delivery of a chatbot service for the purposes of answering generic enquiries.

   As with the online channel, the Service Centre will communicate with regulated parties about their submissions, including sending email notification of a submission such as an arms item transfer.

3 On Day 1, dealer licence holders will be required to submit details of all specified arms items they receive from and sell to firearms licence holders residing in New Zealand. For Release 2.1, this functionality will not be available on the Registry, and instead this record of transactions will be submitted to Te Tari Pūreke via an online form to be completed by the dealer licence holder or their staff. This form will be submitted via the Drupal platform, which is already used by Police (including to allow people to submit information to the 105 channel).

This form will share a subset of the data via an integration with AIS, potentially triggering an automated email notification to the licence holder reminding them of their obligations to register their arms items. An automated matching process for the dealer records will be run against arms items on the Registry. When there is a match, then the transaction is no longer flagged for follow-up. If there is no match after 30 days, then the licence holder will be subject to a manual follow up by the Registry Services team. This information can also be used by Te Tari Pūreke to carry out compliance checks to ensure that the relevant firearms licence holder (who has received or sold arms items) has fulfilled their obligations to register their arms item on the Registry.

4 5 The AIS and NIA will integrate to support both Te Tari Pūreke and the broader Constabulary. This integration will take the form of a daily two-way feed as set out below.

The AIS will pull information about licence holders from NIA. This information will be available as read-only to Te Tari Pūreke staff in AIS, and will be used to support back-office validation and other processes. The AIS will push details of arms items registered to specific firearms licence holders to NIA, where it will be stored against the relevant NIA identity. This information will be used by Constabulary staff for safety purposes, ensuring that frontline staff have accurate and up to date information about arms items that may be present during a call out.

Where the Constabulary requires access to detailed information held in the Registry – such as detailed information about specific dealer licence holder transactions – for the purposes of a criminal investigation, it is anticipated that the Constabulary would make a formal request for this information to Te Tari Pūreke. Te Tari Pūreke would then access AIS or Drupal and generate the reports required for that specific purpose.

6 The Department of Conservation (**DOC**) owns firearms, and their employees who use them as part of their employment are appropriately licensed and endorsed in the same way as other firearms users. DOC has indicated that it would be useful to include its firearms in the Registry. However, a transition period is required to ensure that the Department has robust systems in place to centrally manage registration; and that the Registry can accommodate that there is both Crown ownership and personal possession involved, which is different from other firearms.

7 Other government agencies with a role in managing the import or export of arms items will require some level of access to, or integration with, the Registry. For example, the Ministry of Foreign Affairs and Trade (**MFAT**) will need to be notified when arms items

are being exported out of New Zealand. The NZ Customs Service will have oversight of the importation of arms items into New Zealand, and may need to provide information to Te Tari Pūreke for inclusion in the Registry (which may trigger registration obligations on regulated parties). Access for government agencies is likely to be provided via secure APIs.

8 Te Tari Pūreke needs to be able to use the data held within the Registry – including personal information – for the purposes of generating analytics, including for the purposes of research, operations management, policy planning, and reporting. This will allow Te Tari Pūreke (and the Police more generally) to:

- Identify trends and opportunities for targeted regulatory actions
- Manage data integrity
- Understand Registry and MyFirearms portal usage
- Manage public reporting and Official Information Act requests
- Monitor and manage staff conduct.

In addition to building analytics tools and functionality into the AIS itself, Te Tari Pūreke anticipates that AIS data may be exported to a data warehouse for analytics. Within the data warehouse, AIS datasets could also be combined with other Police datasets, linked with matching keys (such as a licence number or arms item identifier).

5. Summary of IPP application

 No issue

 Relevant, but not serious

 Must be given serious consideration

IPP	Status	Comments
1. Collect only personal information that is necessary for a lawful purpose		Te Tari Pūreke must ensure that it collects only the personal information it needs to meet its lawful purposes. Lawful purposes include administering the Arms Act, operating and maintaining the Registry and associated processes (such as account maintenance and public enquiries) and, to a lesser extent, supporting law enforcement activities of the Police. Most of the personal information to be collected and held on the Registry is mandated by legislation (the Arms Act and its supporting regulations). Te Tari Pūreke must ensure that any personal information it collects that is not mandated by legislation is minimised. We saw no evidence to suggest that Te Tari Pūreke is collecting more information than it needs.
2. Collect personal information directly from the person concerned		Te Tari Pūreke should collect personal information directly from regulated parties where possible. Most of the personal information collected and held on the Registry will be collected directly from the regulated parties concerned, either via the MyFirearms portal or via the Service Centre. Other information – such as information about licence holders – is already held by the Police. Te Tari Pūreke may collect some information from third parties, including collecting information about firearms licence holders from dealer licence holders. This would be permitted on the basis that it is mandated by the Arms Act or regulations (which override IPP 2).
3. Tell people why personal information is required, how it will be used, and who it may be shared with		Te Tari Pūreke must ensure that it is transparent with regulated parties about the collection and processing of personal information for the purposes of the Registry. This transparency will be critical to building and maintaining the trust of the firearms community. At present, Te Tari Pūreke provides piecemeal privacy transparency that may not meet the requirements of the law or the expectations of the firearms community. This will need to be improved. See section 6.7

IPP	Status	Comments
4. Collect personal information in ways that are lawful, fair, and not unreasonably intrusive		Te Tari Pūreke must take care to ensure that the methods it uses to collect personal information from regulated parties are lawful, fair, and not unreasonably intrusive. For the most part, this is addressed by the focus on self-service. In most cases, regulated parties will provide information to Te Tari Pūreke themselves via secure online channels. In these cases, issues of lawfulness, fairness and intrusiveness will not generally arise. However, Te Tari Pūreke will need to be mindful of collection methods in relation to the Service Centre. For example, it will need to inform the public that calls to the Service Centre are recorded. This, and other transparency efforts addressed elsewhere in this PIA will assist Te Tari Pūreke to ensure that the collection of information is fair. **See section 6.7**
5. Take reasonable steps to keep personal information safe and secure		IPP 5 requires Te Tari Pūreke to take reasonable steps to protect personal information. This is not a requirement to implement 'gold standard' or 'bullet proof' safeguards, or to entirely eliminate security risk. That said, in view of the high privacy risk profile identified above at section 2.6, what is 'reasonable' in the context of the Registry is likely to be relatively high. Security is a priority for Te Tari Pūreke , and it has conducted several Security Risk Assessments (and associated activities) in relation to the Registry and Service Centre. However, in this PIA, we identify several other important security considerations s.9(2)(k) OIA [redacted] identity verification, and risks related to sharing information with regulated parties. **See sections 6.1, 6.2, 6.3, 6.4, 6.5, and 6.6**
6. Let people access their information		Regulated parties will have the right to request access to personal information held about them on the Registry (or in other Te Tari Pūreke systems). Ensuring these requests are managed openly and quickly will build and maintain the trust and confidence of the firearms community. For the most part, regulated parties will be able to access their information directly via the My Firearms portal. However, where a regulated party makes a request for information via other channels – such as the Service Centre – Te Tari Pūreke will need to take care to ensure that requests are genuine, and the risk of unauthorised disclosure is mitigated. **See section 6.5**

IPP	Status	Comments
7. Let people correct their information		Regulated parties will have the right to request the correction of personal information held about them on the Registry (or in other Te Tari Pūreke systems). For the most part, regulated parties will be able to update their information directly via the My Firearms portal. However, where a regulated party makes a request to correct information via other channels – such as the Service Centre – Te Tari Pūreke will need to take care to ensure that requests are genuine, and the risk of unauthorised changes is mitigated. **See section 6.5**
8. Take reasonable steps to check personal information is accurate before using it		Te Tari Pūreke must ensure that the information it, and the Police, rely upon to meet their lawful purposes is accurate and up to date. A failure to do so could have significant adverse consequences, both for the individual concerned and the wider community. There are several aspects of the AIS process that could raise accuracy risks. For example, accuracy risks could occur during the manual entry of data into the AIS by Service Centre staff, during the data integration process between AIS and NIA, or in relation to ensuring that the Registry is updated when a regulated party dies. See section 6.10
9. Don't retain personal information for longer that it's needed for a lawful purpose		Te Tari Pūreke must not retain Registry data for longer than it is needed for a lawful purpose. Getting rid of personal information when it is no longer needed reduces the risk of harm in the event of a privacy breach. Te Tari Pūreke has determined that personal information should be retained in the Registry for the duration of the regulated party's life, plus an additional three years. For non-Registry information (such as file notes, call recordings, emails, or chatbot content), Te Tari Pūreke should align its retention periods with the Police's general practice. See section 6.10
10. Use personal information only for the purposes it was collected		Te Tari Pūreke must ensure that it, and the Police more broadly, access and use Registry data only to support the purposes for which it was collected. Effectively managing the risk of scope creep will contribute to maintaining the trust and confidence of the firearms community. For the most part, Te Tari Pūreke will use Registry data for the purposes of administering the Arms Act. This use is required by law. The Police will use some Registry data for law enforcement and safety purposes. This use is permitted by IPP 10. However, Te Tari Pūreke is also contemplating broader uses of Registry data for analytical purposes, including combining Registry data with other Police datasets in a data

IPP	Status	Comments
		warehouse. This will need to be managed with care in order to comply with IPP 10. **See sections 6.1, 6.2, 6.8, and 6.9**
11. Don't disclose personal information, unless an exception applies		Te Tari Pūreke must ensure that it does not disclose Registry data, unless this is one of the purposes for which the information was collected. More importantly, Te Tari Pūreke must manage the risk of unauthorised disclosure, which could cause significant harm to regulated parties and the wider community. This will be critical to maintaining the trust and confidence of the firearms community. This will include managing the risks associated with lawful requests for Registry data, such as requests made under IPP 6 or the Official Information Act. It will also require Te Tari Pūreke to ensure that Registry data used to develop insights or dashboards is properly de-identified before those outputs are released. **See sections 6.5 and 6.8**
12. Only disclose personal information to overseas third parties if it is subject to comparable privacy safeguards		IPP 12 is unlikely to apply to Registry data, because it is highly unlikely that Te Tari Pūreke will need to disclose this data to overseas agencies. It should be noted that IPP 12 does not apply to the sharing of personal information with cloud-based service providers that will process or store data overseas, because such sharing is not deemed to be a "disclosure" for the purposes of IPP 11.
13. Only assign unique identifiers if you need to, and don't assign another agency's unique identifier		Te Tari Pūreke will not use any unique identifiers assigned by other agencies. It will use the licence number and AIS account number, and will need to decide which of these unique identifiers it will use as its primary identifier.

6. Privacy risk and opportunity assessment

6.1 Managing service provider risk

Te Tari Pūreke has procured the services of several third-party service providers to deliver the Registry and Service Centre. As such, Te Tari Pūreke is entrusting data – including personal information – to these service providers, but remains liable for that data while it is in their care. For this reason, it is essential that each service provider gives appropriate contractual and other assurances in relation to data ownership, protection, access, and use.

6.1.1 Contractual assurances from service providers

We have reviewed the contractual agreements between Police and the two primary service providers being used for the AIS project – Objective and Genesys. In addition, because the data processed within both Objective and Genesys will be hosted by Amazon Web Services (**AWS**), we have reviewed the universal Service Terms provided by AWS.[6] These Service Terms apply to all services AWS offers, including cloud storage services.

In this review, we are assessing how well each contract reflects the status of the parties under the Privacy Act (as data controller or data processor[7]), how well the documents ensure that controllers retain control of the data, and how well the documents address the privacy and security assurances that are now standard in these sorts of arrangements. Note, this is not a security assessment; this assessment is limited only to the contractual assurances given. On the basis of this assessment – summarised in Fig. 2 below – it is our view that the service provider contracts contain the appropriate assurances.

Figure 2 – High-level review of privacy assurances

Assurance	Objective	Genesys	AWS
1. The customer will own the rights to the information processed on their behalf.	**Yes** – clause 12.1 - Provider is only holding information as Police's agent	**Yes** – clause 14.2 – Police retain ownership of and all IP rights in information	**Yes** – clause 1.1 of DPA states that AWS will act as a processor in relation to customer data
2. The service provider will use the information only to deliver the services or on the	**Yes** – clause 12.2(a) and (b) – Provider will only use information to the extent	**Yes** – clause 14.1 – Provider will only use information in accordance with	**Yes** – clause 2 of DPA states that AWS will process customer data only in accordance

[6] AWS Service Terms and Data Processing Addendum.
[7] The terms "controller" and "processor" are not used in the Privacy Act, but have been borrowed from the EU General Data Protection Regulation (GDPR) on the basis that they provide a more useful and clear shorthand to refer to the various parties in a service provider relationship. Section 11 of the Privacy Act states that where an agency (the processor) holds or processes personal information solely on behalf of another agency (the controller), the controller is deemed to hold the information, and is therefore liable for it under the Privacy Act.

Assurance	Objective	Genesys	AWS
instructions of the customer, unless required by law.	necessary to provide the services and will not use it for its own purposes. Further clause 10.1 prohibits the provider form using information for analytics purposes	Agreement and not for other purposes/its own purposes	with documented instructions
3. The service provider will limit access to the information to those who need to do so to deliver the services.	**Yes** – clause 12.1(a) – Provider personnel will only have access to information if necessary to provide services	**Yes** – clause 14(1)(a)(vi) – Provider will take technical and organisational measures to ensure no unauthorised access	**Yes** – clause 4 of DPA states that AWS will restrict its personnel from processing customer data without authorisation
4. The service provider will protect the information with adequate organisational and technical security measures.	**Yes** – clause 12.2(f), 12.5, 12.6(b) – Provider undertakes to protect information from a security breach, prevent unauthorised access, use or disclosure or loss and undertake regular security testing	**Yes** – clause 14.1(a)(i),(vi),(vii) and (viii) - Provider undertakes to keep information secure and prevent unauthorised access, use or disclosure or loss	**Yes** – clause 5 of DPA states that AWS will implemented and maintain technical and organisational measures to ensure network security, physical security, access controls, and security testing
5. The service provider will not disclose the information to a third party, unless authorised by the customer or required by law.	**Yes** – clause 12.2(c) – Provider will not disclose information to a third party and clause 12.3 will provide notice if information required to be disclosed by law	**Yes** – clause 14(1)(a)(i)-(iii) and 14(b) and (c) – Provider will only disclose in accordance with agreement unless required to by law	**Yes** – clause 3 of DPA states that AWS will not disclose customer data to any third party unless required by law (in which case it will attempt to redirect requests to customer)
6. The service provider will return and destroy the information on request from the customer or at the conclusion of the services.	**Yes** – clause 11.8 – Police can request return or destruction of information at any time during agreement term.	**Yes** – clause 14.5 – all data to be deleted on termination or expiry and once Police no longer using relevant environment	**Yes** – clause 1.15 of Service Terms states that AWS will delete all content following closure of AWS account, and clause 14 of DPA states that AWS will return or delete customer data on termination
7. The service provider will notify the customer immediately of any privacy or data breach that affects the customer's information.	**Yes** – clauses 12.8 and 12.9 – Provider will immediately notify Police of any privacy breach (incl suspected or threatened breach)	**Yes** – clause 14.3 - immediate notification of actual or suspected breach	**Yes** - clause 9 of DPA states that AWS will notify customer of breach without undue delay, and will take steps to mitigate adverse effects

Clause 12.7 of the agreement with Objective provides Te Tari Pūreke with the ability to request a copy of Objective's own privacy policy to enable it to assess whether Objective is complying with the privacy obligations set out at clause 12.6 of the agreement. We have reviewed this policy and consider it to be acceptable. The policy properly distinguishes between Objective as a data processor (in relation to the data it processes as a service provider, which would include Registry data) and as a data controller (in relation to data it collects and processes about users). The ways in which Objective collects and processes user data appear to be industry standard and appropriate.

6.1.2 Data storage arrangements and jurisdictional risk

Jurisdictional risk occurs when personal information is subject to the laws of the country where a cloud service provider stores, processes or transmits the information. Jurisdictional risk may lead to situations which are harmful to New Zealand's national interests or inconsistent with New Zealand's laws, as it is not possible to fully contract out of the laws of another country. While section 23 of the Privacy Act states that actions taken by an agency in relation to information held overseas do not breach the IPPs if they are required under the law of another country, such actions may nonetheless cause harm to agencies and their people.

Jurisdictional risk is generally determined by assessing three criteria – the sufficiency of a country's privacy framework, the scope of a country's interception or surveillance laws (lawful access), and the robustness of a country's legal institutions and oversight mechanisms.

While personal information being processed may transit several countries, both Objective and Genesys will store Te Tari Pūreke data at rest in **Australia**.[8] Australia has a privacy framework in place that is more robust than NZ (and is currently undergoing significant reform). Recent expansions to the lawful access framework are focused on the interception of encrypted communications or devices, not enterprise data. In view of the strong oversight mechanisms, the likelihood of Australian Government agencies accessing Te Tari Pūreke data stored in Australian-based servers is low. On this basis, the jurisdictional risk for Australia is acceptable.[9]

AWS intends to build new data centres in NZ,[10] which will allow the company to establish a NZ AWS region. Te Tari Pūreke has confirmed that it will move its data to the NZ AWS region once this is available. This will significantly reduce jurisdictional risk, provide further assurance to the firearms community in relation to the protection of their data, and help address Māori data sovereignty concerns.

[8] Note clause 12.4 of the Objective contract prohibits the storage of data offshore without Police prior written consent.
[9] While it was reported in 2020 that the Parliamentary Service had stalled a move Microsoft 365 on the basis of the Australian decryption law, it must be noted that this was based on the Service's specific risk profile. The Service delivers communications, data and technology infrastructure services to Parliament, the DPMC and an number of other government agencies within the parliamentary precinct. As part of this function, the Service must maintain parliamentary privilege and consider national security implications of exposing parliamentary communications to jurisdictional risk.
[10] https://www.nzherald.co.nz/business/infrastructure-data-cloud-centres-with-golden-lining/M6YWTF5JSBDITKKVRQCFDAL5OI/.

6.2 Governance of the Registry and its data

A strong governance framework sits at the heart of the principle of **Kaitiakitanga**. This will enable Te Tari Pūreke to set a clear direction for the management of personal information and ensure it remains accountable for all the information in its care. This is about governance over information, people, process and change. There are several important components to a governance framework:

1. **Data ownership** – Assigning ownership to the various categories of personal information collected and held by Te Tari Pūreke for the purposes of managing the Registry and associated processes will minimise the risk of scope creep, by ensuring that data uses, data sharing, and changes to systems or processes are signed off at the right level. This would include ensuring that Constabulary access to Registry data is appropriate.

2. **Accountability measures** – Establishing measures to ensure that Te Tari Pūreke remains accountable at all times for the ways it accesses, processes, and shares personal information will increase the trust and confidence of the firearms community and increase the likelihood that data misuse will be both identified and prevented.

3. **Escalation rules** – Setting clear and consistent escalation pathways for privacy and security risks and events (such as complaints and privacy breaches) will minimise the adverse consequences of these risks and events.

4. **Strong leadership** – Ensuring that Te Tari Pūreke's senior leadership team develops and conveys strong and clear privacy messages to all staff will build a privacy and security culture. This will create a safer environment within which personal information can be used to meet the Te Tari Pūreke's legislative mandate.

5. **Privacy expert support** – Te Tari Pūreke will need to consider how best to ensure that it receives the ongoing privacy expert support it needs to ensure effective privacy governance and accountability. It will need to decide, in view of the high privacy risk profile identified above at section 2.6, whether it is sufficient to rely solely on Police's centralised Privacy Team, or whether additional Te Tari Pūreke privacy resource (such as a Privacy Champion) will be required.

Rec-001: Assign Data Owners for the personal information the Te Tari Pūreke holds, to reduce the risk of scope creep.

Rec-002: Establish and communicate clear escalation rules for Te Tari Pūreke privacy and security risks and events.

Rec-003: Consider how best to ensure Te Tari Pūreke receives the ongoing privacy expert support it needs to manage its specific privacy risk profile and ensure the protection of the sensitive personal information it holds.

6.2.1 Monitoring access logs to increase accountability

Logging user activity within the Registry and then carrying out monitoring and audit activities to ensure that activity is appropriate is a key control to both detect and deter unauthorised access by authorised users, such as employee browsing. It will provide a level of assurance and comfort to the firearms community that their personal information is not at risk.

s.9(2)(k) OIA [redacted]

s.9(2)(k) OIA [redacted]

s.9(2)(k) OIA [redacted]

s.6(c) OIA [redacted]

In terms of processes and thresholds around monitoring, we recommend Te Tari Pūreke to implement a similar approach as is currently taken by Police to monitoring access to NIA. This

s.9(2)(k) OIA [redacted]

Rec-005: Where appropriate and practicable, implement a similar approach for AIS monitoring and audit as is currently applied to the NIA.

We also recommend that the monitoring should target s.9(2)(k) OIA [redacted]

s.9(2)(k) OIA

[redacted]

6.3 Security as foundation of trust

Te Tari Pūreke has carried out number of Security Risk Assessments (**SRAs**) in relation to the AIS project. This includes a comprehensive assessment of the Objective Regworks platform as part of release 1, which has subsequently been updated to include aspects specific to Release 2.1. In addition, an SRA on the Service Centre has been completed. We have reviewed these SRAs and, although a technical security assessment is out of scope of this PIA, security is an obligation under IPP 5 of the Privacy Act, as well as a key component of the Privacy by Design principles and the principle of **Kaitiakitanga**.

In view of the high privacy risk profile identified above at section 2.6, it will be critical for Te Tari Pūreke to ensure that all recommended security controls are in place on Day 1. Security must be viewed as a core requirement before launch, not an eventual add-on. Teething problems will inevitably arise as the Registry is launched, particularly because new staff will be using new systems and exercising newly gained knowledge. This is when human error is most likely to occur. Ensuring that technical and organisational security controls have already been implemented will mitigate this risk. This will also protect the Registry and its data at a time when the system will be under significant scrutiny from the firearms community.

s.9(2)(k) OIA

[redacted]

s.9(2)(k) OIA

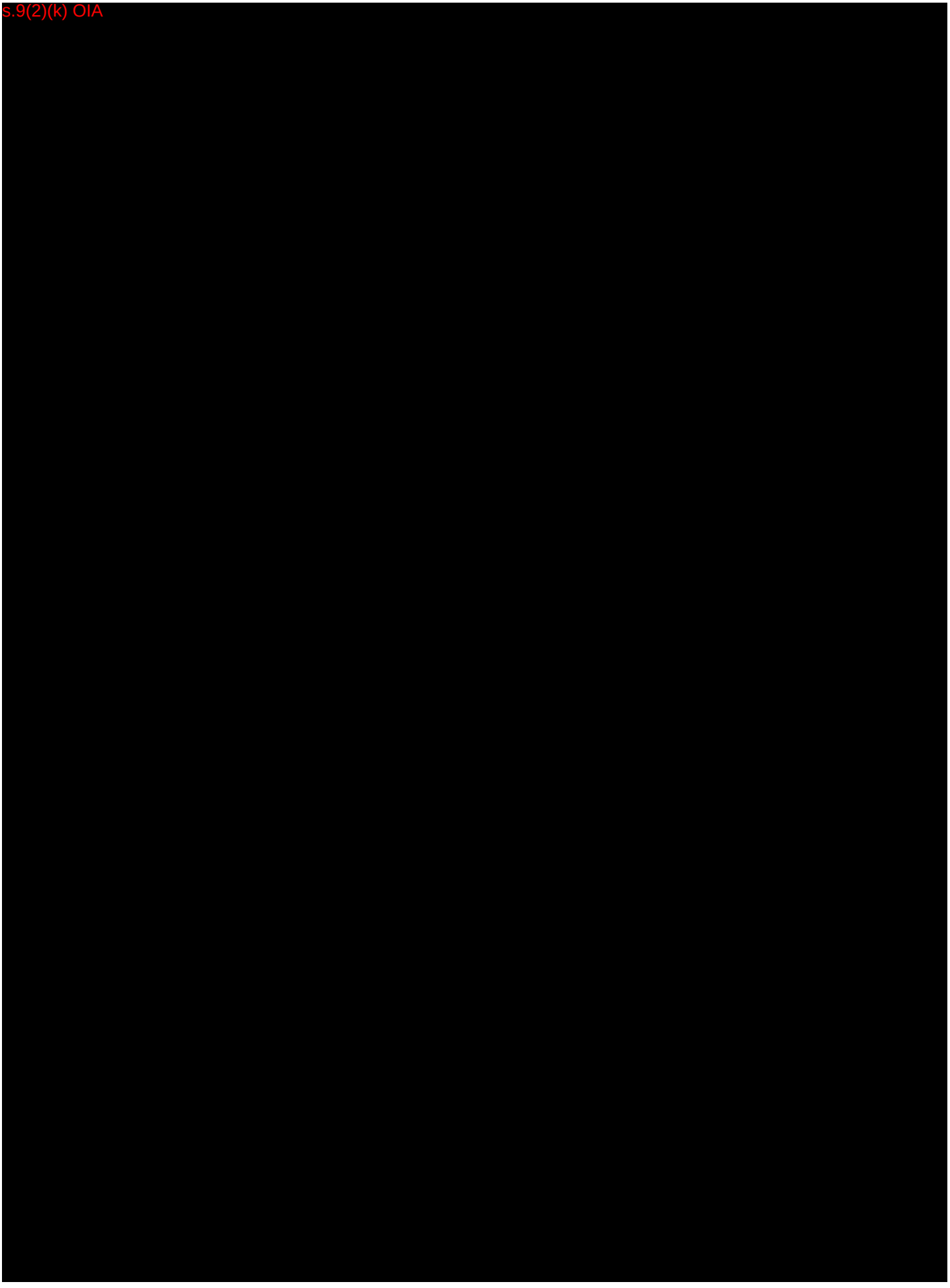
[redacted]

s.9(2)(k) OIA

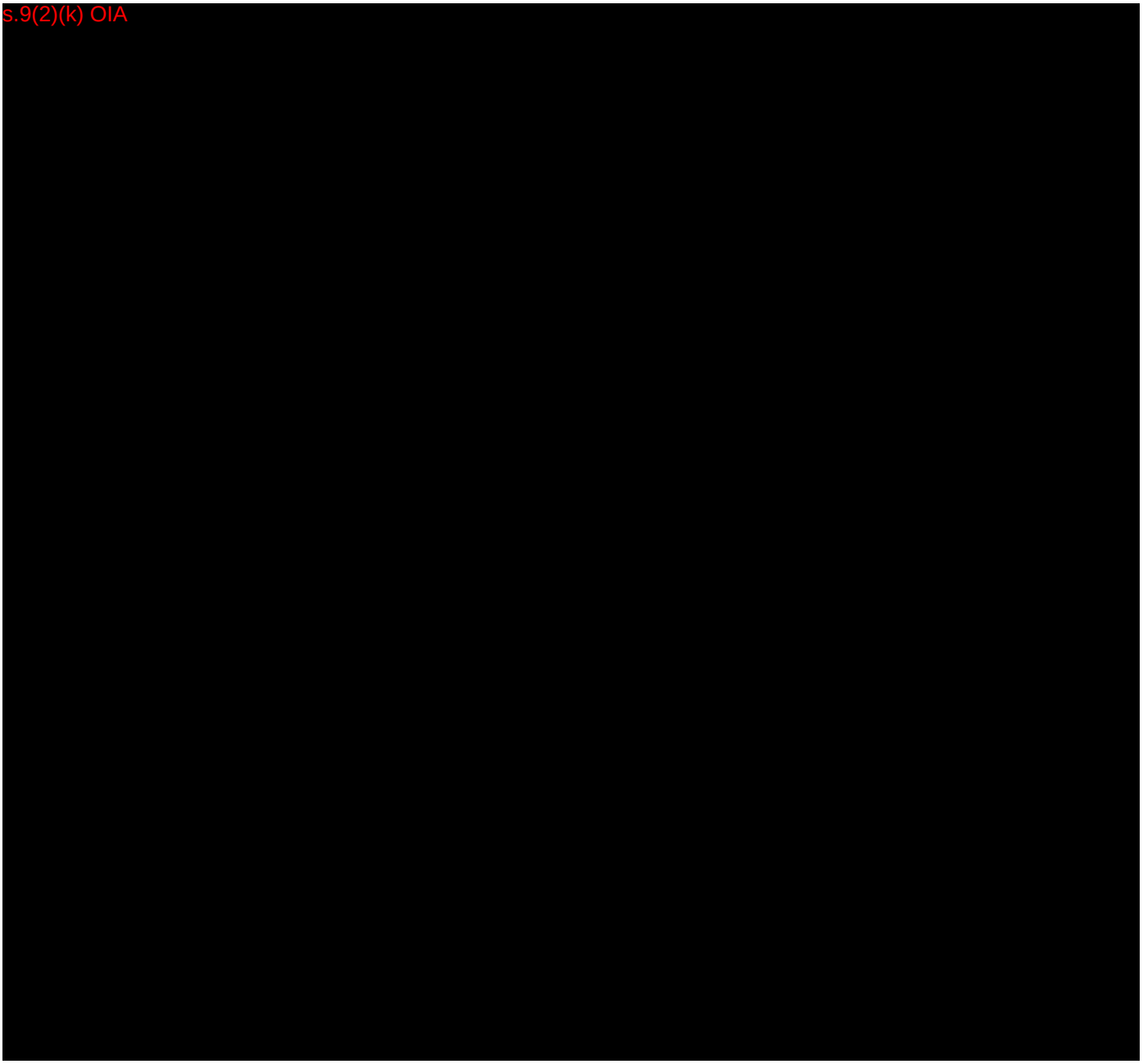
s.9(2)(k) OIA

s.9(2)(k) OIA

s.9(2)(k) OIA



s.9(2)(k) OIA



6.5 Enabling safe public access to data

Regulated parties have a legitimate expectation – and a right under IPP 6 of the Privacy Act – to access the information held about them on the Registry. It is important that Te Tari Pūreke enables regulated parties to exercise this right. However, due to the sensitivity of the personal information held in the Registry, and the potentially serious harm an unauthorised disclosure could cause, Te Tari Pūreke will need to take great care to ensure that Registry information is shared only with the relevant licence holder.

[11] Similar software is used by tertiary education providers for remote exam proctoring. It is accepted that this control is invasive, and Te Tari Pūreke would need to balance this against privacy obligations to staff, including complying with IPP 1 and IPP 4 in respect of collecting personal information about them.

For this reason, Te Tari Pūreke may need to take a more restrictive approach to managing access to personal information than other agencies might. As noted below, it is already developing such an approach, including directing more sensitive requests to the Police's existing and more formal centralised request process with its robust identity verification processes. While this may not result in the best customer experience, this approach is justifiable in the context of the risk of unauthorised disclosure in the case of the Registry.

Further to this, Te Tari Pūreke has a legitimate need to communicate with regulated parties about submissions through MyFirearms or the Service Centre. Again, the sensitivity of the subject matter of these communications (for example, relating to the submission of arms items to the Registry), Te Tari Pūreke needs to take great care to manage the risk of disclosing sensitive information to the wrong person.

Firearms licence holders with validated MyFirearms accounts will of course generally be able to access all the information they need via the MyFirearms portal. This will assist Te Tari Pūreke to meet its obligations under IPP 6 in a way that is secure, noting that the licence holder will need to login to their account using their RealMe identity. However, dealer licence holders will not be able to access their information via MyFirearms, and all regulated parties may from time to time need to make requests to Te Tari Pūreke via other means, including the Service Centre.

6.5.1 Identity verification

Te Tari Pūreke has correctly identified that a key risk the Service Centre faces is that individuals seeking access to information about other people's firearms, including their location, might attempt to deceptively obtain this information via the Service Centre via impersonation or social engineering tactics.

Te Tari Pūreke has decided to base its Service Centre identify verification processes on the Identification Management Standards published by the DIA. These define three different authentication factors - something you know (such as a password); something you have (such as a one-time code generator such as Microsoft Authenticator) and something you are (such as biometric information).

Only the first category of authentication information (something you know) will be available to Service Centre staff on Day 1. This category can be further split into information the caller will know but that others might also know, and information that should only be known to the caller and Te Tari Pūreke.

To help mitigate this risk, Te Tari Pūreke has developed assessment criteria which take into account considerations such as the nature of the submission and the risks of misidentification. These criteria will inform the level of identity validation that is required for the relevant interaction. The highest risk is where information about a licence holder's firearm(s) and location might be given to a third party.

To further mitigate this risk a number of controls are under consideration by Te Tari Pūreke. These include robust call scripting and policies setting out what steps must be taken, and conditions put in place, before personal information is disclosed to a caller.

We have reviewed draft copies of key Service Centre policies relating to identity verification and make the following observations:

- **Telephony Information Release Policy**
  This is aimed at preventing the release of sensitive information to an unauthorised party. It sets out parameters for what information can and cannot be disclosed over the phone after identity verification has been completed. For example, a caller will not be provided with information about previously registered arms items over the phone, to avoid mistakenly disclosing this sensitive information to the wrong person.

  As noted above, if a caller wishes to request access to, or correction of, the information about them relating to registered arms items, they will be required to submit a request via the Police's usual process for managing Privacy Act requests. This will allow Police to manage these sensitive requests with care, take any additional steps required to verify the identity of the requester, ensure the correct information is released, and ensure that the information is released in a safe and secure way (such as to a verified email address). In view of the sensitivity of this information and the fact that most firearms licence holders will be able to access their own information via MyFirearms, this is an appropriate process to balance access rights against disclosure risk.

- **Regulated Party Telephony Validation Policy**
  This outlines the identity verification policy for Service Centre staff and reflects Te Tari Pūreke's obligation under section 57 of the Privacy Act to ensure it does not release personal information unless it is satisfied of the person's identity. It notes the failure to verify can put individuals at risk of harm and provides clear guidance to staff, requiring five validation questions to be asked and answered correctly.

s.9(2)(k) OIA

[redacted]

s.9(2)(k) OIA

[redacted]

Rec-011: Consider developing a process to flag and manage a known risk to a firearms licence holder's account, on the basis of possible impersonation attempts.

- **Third Party Approval Policy**
  This addresses the scenario where someone is calling on behalf of a regulated party to seek information about that regulated party, and reflects the Te Tari Pūreke's obligation under section 57(d) of the Privacy Act not to release personal information in these circumstances unless it is satisfied the representative is properly authorised.

  The policy only allows disclosures of limited information, and only when the regulated party is present and able to both have their identity validated and provide a verbal authorisation for their representative to receive information. Any such authority will only last for that specific phone call. The only exception to this is if the caller holds a Power of Attorney in respect of the regulated party, in which case the policy notes that the standard Police process is to be followed.

  In some situations, the regulated party may not be able to authorise the third party in the way set out in the policy. For example, they may be unwell or have a disability which means they cannot participate in the validation process. There will not always be a Power of Attorney in existence in these scenarios. In addition, the policy will need to accommodate the scenario where the executor or administrator of an estate of a deceased person who was in possession of a firearm is required to notify Te Tari Pūreke of this (and any relevant transfer), and to provide both proof of death and their authority.

  It may be that, practically speaking, the best way to deal with third parties without a Power of Attorney or proof of Executorship is to escalate all such calls to a Team leader or other more senior Service Centre staff member to deal with on an ad hoc basis. However, we recommend that Te Tari Pūreke should review these and any other possible scenarios, and consider providing additional guidance to staff in relation to managing common scenarios of this sort.

Rec-012: Consider developing guidance for Registry Service Centre staff to identify and manage difficult request scenarios, including requests from representatives.

Further, ensuring staff feel supported to 'hold the line' with difficult callers, or where they suspect something is unusual, will also support effective identification verification. This should include ensuring that performance measures for Service Centre staff are not solely linked to metrics such as numbers of callers verified or customer experience scores.

Rec-013: Support Registry Service Centre staff to take a robust approach to managing the identity verification process, including by avoiding performance measures linked solely to numbers of callers verified or customer experience scores.

6.5.2 Managing dealer requests

On Day 1, dealer licence holders will not be able to use MyFirearms to make submissions to the Registry. Instead, as outlined above, they will make submissions to the AIS via Drupal. This will include notifying Te Tari Pūreke of transactions for specified arms Items on a regular basis. Because dealer licence holders will not be able to easily access the information they have submitted, there will be a period in which they may need to make ad hoc requests to Te Tari Pūreke for extracts from the dealer solution, showing the transactions they have submitted (**dealer reports**).

As noted above, dealer licence holders would be entitled to request this information under IPP 6 of the Privacy Act (if they are not incorporated entities) or the Official Information Act (**OIA**). However, the compilation of reports that identify the firearms transfers specific firearms licence holders have been involved in will create a significant privacy risk. For this reason, the AIS project team is actively considering what controls could be put in place to meet the needs of dealer licence holders while mitigating the privacy risk.

s.9(2)(k) OIA

Tari Pūreke's behalf.

In our view, data minimisation will be one of the most effective controls to minimise risk in relation to dealer reports. However, the Police Legal Team has taken the view that Te Tari Pūreke is not entitled to withhold any information from a dealer licence holder, in view of the fact that this is information that individual has submitted to Te Tari Pūreke. Before making a decision on which controls are feasible, it would therefore be prudent to engage with the dealer community to understand what information they need these dealer reports to include, noting that Te Tari Pūreke is looking to meet their needs in a way that protects the privacy and safety of firearms licence holders. Once dealer views are obtained, Te Tari Pūreke can finalise the process for managing dealer report requests.

Rec-014: Engage with the dealer community to explain the risks associated with releasing dealer reports, and to fully understand the needs of dealer licence holders, before finalising the possible controls to manage the privacy risk associated with this process.

6.5.3 Communication channel risks

Te Tari Pūreke will also need to communicate with regulated parties about the submissions they make on MyFirearms or via the Service Centre. Some of these communications will be automated as part of the MyFirearms submission process. In other cases, communications may be initiated by the Service Centre after firearms licence holders have made manual submissions. For example, Te Tari Pūreke will need to provide acknowledgements to firearms licence holders that submissions (for example new arms item registrations or transfers) have been received and are being processed. Te Tari Pūreke will also need to update firearms licence holders about the progress of their submissions in the system.

s.9(2)(k) OIA

[redacted]

Rec-015: Ensure routine customer service communications to firearms licence holders contain the minimum personal information possible to achieve their goal.

6.6 Privacy training for Te Tari Pūreke

Te Tari Pūreke staff (and particularly Service Centre staff) will need to be given appropriate training in privacy and security prior to Day 1. The establishment of new processes, using new systems, operating under new legislation, and with new staff creates a particularly high risk of error in the initial days and weeks of operation. Providing staff with clear privacy and security training and guidance will help reduce this error rate.

We understand that all staff will complete the standard Police training modules on privacy and security. However, in view of the high privacy risk profile identified above at section 2.6, we recommend additional Registry-specific privacy and security training be provided to all Te Tari Pūreke staff prior to Day 1. Ideally, this will be provided on an in-person basis to allow for interaction and questions to be asked.

Ensuring that Service Centre staff are equipped to detect and resist attempts by individuals to get around identity verification processes should be part of any training provided. Being given the tools to enable staff to identify and resist attempts at social engineering and manipulation will provide an additional layer of protection for the personal information held in the Registry. Te Tari Pūkere has confirmed that Service Centre staff will also be required to complete a specific training module on ID verification.

Rec-016: Develop and deliver Te Tari Pūreke -specific privacy and security training to all staff prior to Day 1.

6.7 Privacy transparency

All agencies are required by IPP 3 of the Privacy Act to provide privacy notices to individuals about the collection and processing of personal information. However, for the Te Tari Pūreke privacy transparency is more than a simple compliance obligation. Ensuring open, clear and effective privacy transparency for regulated parties will be an important way to build and maintain the trust and confidence of the firearms community. It is a foundation of the principle of **Mana Whakahaere**, and an effective way to communicate how Te Tari Pūreke is meeting the principle of **Kaitiakitanga**.

Te Tari Pūreke currently delivers privacy transparency in several ways, as follows:

- A **privacy policy** on the Te Tari Pūreke website[12] relates specifically to the collection and processing of personal information about users of the Te Tari Pūreke website and MyFirearms portal. The policy focuses on website user data, such as device information and usage information generated through cookies. It also explains how Te Tari Pūreke uses web analytics (such as Google Analytics). It does not address the collection and processing of personal information about the regulated community for the purposes of the Registry.

- The **MyFirearms Terms of Use**[13] provide a short collection notice in relation to the collection and processing of personal information for the purposes of administering the Arms Act. It notes that Police may use personal information about regulated parties to carry out its lawful functions, and then directs individuals to the Police's general privacy statement for more information.

[12] https://www.firearmssafetyauthority.govt.nz/about-us/privacy.
[13] https://www.firearmssafetyauthority.govt.nz/about-us/myfirearms-terms-use.

- **Police's general privacy statement**[14] is necessarily broad. It outlines the full scope of Police's activities, and provides individuals with notice of the broad range of purposes for which personal information held by the Police may be used or shared.

While it is quite correct – and appropriate – to inform regulated parties that Registry data may be made available to the Police for a range of purposes, the series of notices outlined above do not do justice to the many controls Te Tari Pūreke has put in place to ensure that Registry data is protected, and used only for limited purposes by the Constabulary. The current approach indicates that there is no separation between the Regulator and the Constabulary, and will not build trust and confidence with the firearms community.

In view of the high privacy risk profile identified above at section 2.6, and the unique processes required to manage privacy requests, Te Tari Pūreke should consider developing a standalone privacy statement for the Registry, aimed at providing assurances to the firearms community that Registry data will be managed with care and used only for a limited set of legitimate regulatory and law enforcement purposes. At the very least, Te Tari Pūreke should consider developing a new section in the Police's general privacy statement that relates specifically to the management of Registry data.

Rec-017: Develop a standalone privacy statement for the Registry, aimed at providing assurances to the firearms community that Registry data will be managed with care and used only for a limited set of legitimate regulatory and law enforcement purposes.

6.8 Safely leveraging Registry data

It is quite reasonable for Te Tari Pūreke to consider how Registry data can be leveraged to inform data analytics, research and innovation that will assist with policy planning, service delivery improvements, and even broader research that can benefit the community. It is accepted that public sector agencies need to better harness and exploit the data and insights they hold for the benefit of New Zealanders.

The DPUP articulates this concept through the principle of **Mahitahitanga** - working as equals to create and share valuable knowledge. This incorporates sharing data in ways that decrease the burden on service users and ensure the best outcomes for people and their communities, and also ensuring that de-identified data can be used for research and evaluation. The Privacy Act also permits the use of personal information for statistical and research purposes, provided that it will not be published in an identifiable form.

However, DPUP and the Privacy Act require that the use of data for innovation, research and development, reporting and policy purposes is managed with great care, to ensure that leveraging the benefits of data does not come at the cost of individual privacy. For Te Tari Pūreke, the need to put rules and boundaries in place around the broader uses of Registry data is even more acute. The aggregation of information about regulated parties could significantly

[14] https://www.police.govt.nz/about-us/how-we-manage-personal-information?nondesktop.

increase the risk of harm in the event of a privacy breach, particularly where such information is aggregated in relation to a single firearms licence holder, or dealer licence holder.

As outlined above in section 4.2, in addition to building analytics tools and functionality into the AIS itself, s.9(2)(k) OIA [redacted] Controls to enable Te Tari Pūreke and Police to use Registry data in a safe way will include:

s.9(2)(k) OIA [redacted]

Rec-018: Put controls in place to mitigate risks associated with using Registry and dealer transaction data for broader analytics purposes.

6.9 Risk-assessing new technological features

The Privacy Commissioner has a keen focus on the privacy implications of new and innovative technologies, and particularly technologies that incorporate algorithms, artificial intelligence and machine learning, profiling and analytics utilising big data, automated decision-making, and biometrics. There is a concern that such technologies can erode the checks and balances in place in manual processes, create opaque decision-making, exacerbate issues such as unwanted bias and discrimination, and ultimately increase the risk of harm to individuals.

s.9(2)(k) OIA [redacted] such as Objective and Genesys s.9(2)(k) OIA [redacted]

[15] https://www.stats.govt.nz/integrated-data/how-we-keep-integrated-data-safe/#five.

s.9(2)(k) OIA

[redacted]

s.9(2)(k) OIA

[redacted]

It will be critical for ongoing trust and confidence in the AIS – and compliance with the Privacy Act by Te Tari Pūreke – to ensure that the adoption of technological features, or the development of new features, is carefully risk assessed, including though the use of PIAs, customer focus groups, and a robust authorisation process that ensures such features are approved at the right level before being utilised. This would need to include ensuring that Te Tari Pūreke is made aware of the algorithms that underpin any automated features that could have an impact on individuals.

s.9(2)(k) OIA

[redacted]

6.10 Other compliance issues

In section 5, we identified several other issues in relation to compliance with the IPPs. These issues should also be addressed by the AIS project to ensure that all the IPPs have been adequately considered and accommodated.

6.10.1 Reasonable steps to ensure accuracy

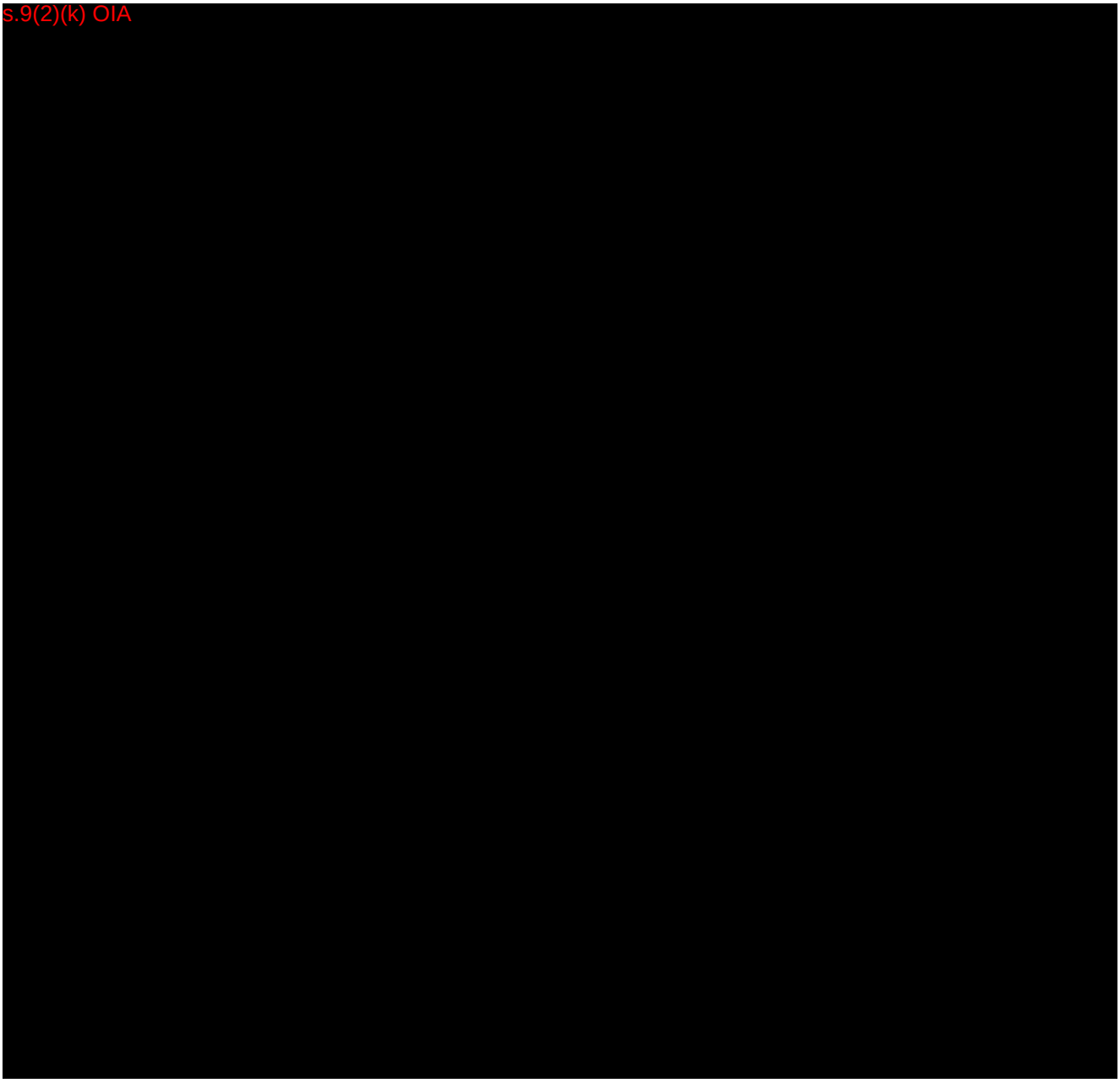
IPP 8 is primarily engaged when an agency intends to use or disclosure personal information for a particular purpose. However, if personal information is likely to be accessed and used regularly

[16] https://www.genesys.com/en-gb/capabilities.

as part of an agency's BAU processes, IPP 8 may require an agency to have ongoing, repeatable processes in place to ensure that the information remains accurate, up-to-date, and complete.

The personal information contained in the Registry will be accessed and used regularly as part of Te Tari Pūreke's BAU processes. The data, including what arms items are in the possession of a particular regulated party, is also likely to be accessed and used regularly by the Constabulary. In some cases, the information could be used in ways that have a negative impact on the individual concerned (such as in relation to specific law enforcement or regulatory activities). For this reason, Te Tari Pūreke will need to put reasonable steps in place to ensure that the personal information in the Registry remains accurate, up-to-date, and complete.

s.9(2)(k) OIA



[17] https://privacy.org.nz/publications/statements-media-releases/notable-increase-in-data-breaches-reported/.

6.10.2 Data retention rules

Te Tari Pūreke must not retain Registry data for longer than it is needed for a lawful purpose. Getting rid of personal information when it is no longer needed reduces the risk of harm in the event of a privacy breach, and minimises the risk of scope creep or other data misuse.

Te Tari Pūreke has determined that personal information should be retained in the Registry for the duration of the regulated party's life, plus an additional three years. Because this retention period will be a requirement of the regulations, this will override IPP 9 of the Privacy Act. That said, this retention period appears to be reasonable for the purposes of operating the Registry and administering the Arms Act.

For non-Registry information (such as file notes, call recordings, emails, or chatbot content), Te Tari Pūreke should align its retention periods with the Police's general practice, including compliance with the relevant General Disposal Authority. Whatever retention periods are selected, Te Tari Pūreke will need to ensure that these are complied with in respect of the AIS and the other platforms used to manage the Registry (such as Genesys).

Rec-021: Develop data retention rules for non-Registry information held by Te Tari Pūreke that align to Police's general practice, and ensure Te Tari Pūreke systems are configured to comply with these retention rules.

Appendix 1: Information gathering

Key stakeholders interviewed

- Paul Robinson – Senior Project Manager, Registry Management
- Annabel Fordham – Chief Privacy Officer, NZ Police
- Colin Trotter – Principal Privacy Advisor, NZ Police
- s.9(2)(a) OIA
- s.9(2)(a) OIA
- Kathryn McCarrison – Project Manager, Registry Management
- Phil Hanlon - Director Change, Te Tari Pūreke
- Richard (RJ) Wilson - Director Operations, Te Tari Pūreke
- s.9(2)(a) OIA
- s.9(2)(a) OIA
- s.9(2)(a) OIA
- s.9(2)(a) OIA

Key documents reviewed

- Firearms Registry Regulations Cabinet Paper (15 December 2022) Final
- Selections of the Report: Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019
- NZ Police, Proposals for new regulations under the Arms Act 1983 (August 2022)
- Firearms Registry Consultation – Submissions Analysis (10 November 2022)
- High Level Requirements – Day 1 – AIS Release 2 – Registry (14 October 2022)
- Detailed Design – Business Configuration (14 December 2022)
- Detailed Design – Arms Information System (20 February 2023)
- Contact Centre DIA Identification Risk Assessment – v0.4 (24 January 2023)
- NZP Service Centre Assessment (31 January 2023)
- Service Centre PID (January 2023)
- Te Tari Pūreke Contact Centre Service Model – v3 (December 2022)
- Te Tari Pūreke Service Desk Statement of Work (14 February 2023)
- Spark TaaS Agreement
- Objective Agreement
- Objective Privacy Policy (last updated 11 July 2022)
- AWS Universal Services Terms
- AIS Security Risk Assessment (November 2022)
- Draft SRA FIS Contact Centre (20 February 2023)
- NIA Privacy Impact Assessment (March 2020)
- ATP Release One PIA – v3.0 (25 October 2022)
- Police Policy - Acceptable use of information and ICT
- Police Policy – Code of Conduct
- Police Policy – Flexible employment
- Police Policy – Information security
- Police Policy – Information and records management
- Police Policy – WFH Guidance