Simply Privacy

Ministry of Business, Innovation & Employment
Hīkina Whakatutuki

Independent Privacy Impact Assessment on Business Connect

Version 1.0
27 April 2023

By Daimhin Warner
Principal & Director
Simply Privacy Ltd

Contents

Version	Date	Author	Comments
0.1	20 March 2023	Daimhin Warner	First draft for consultation
1.0	27 April 2023	Daimhin Warner	Final version, incorporating stakeholder feedback

Executive summary

This is an independent Privacy Impact Assessment (**PIA**) on the Business Connect Platform. The purpose of Business Connect is to provide business and government with a common platform to enable government agencies to digitise and streamline business services and interactions across central and local government.

This PIA has three primary purposes. The first is to identify the privacy risks MBIE is responsible for and assess whether they have been adequately managed. The second is to identify the privacy risks associated with using service providers, including cloud-based providers that might store or process personal information overseas, and assess whether these have been properly addressed in the complex contractual approach taken. The third is to identify how MBIE can develop Business Connect tools and functionality to better support GSPs to meet their own privacy obligations.

The PIA is intended to build trust with all Business Connect stakeholders, enabling the growth and evolution of the platform in a way that will meet the needs of GSPs and the business community while protecting and respecting the personal information processed through it.

Both Business Connect and the government services it facilitates are targeted at businesses, not individuals. This means that, for the most part, the information collected via Business Connect will be about incorporated businesses, and therefore not subject to the Privacy Act. On this basis alone, the privacy risk profile might be considered nominal. However, there will be several scenarios in which Business Connect, and the GSPs using it, will be collecting personal information that is subject to the Privacy Act. This will elevate the overall privacy risk profile for Business Connect, and the findings and recommendations made in the PIA reflect this.

Recommendation	Page
customer of a privacy breach must be made by either the Host Agency or affected Client Agency, not by Datacom or any other service provider.	
Rec-005: MBIE **should** request that Pega amend the Pega EULA to include a clause relating to the return and/or destruction of Business Connect data on termination of the services.	36
Rec-006: MBIE **could** update the Business Connect Product Overview to reflect the findings of this PIA and provide better clarity to GSPs on the roles and responsibilities of all stakeholders under the Privacy Act.	37
Rec-007: MBIE **should** consider moving Business Connect data at rest to AWS data centres within the NZ AWS region when this option is available.	38
Rec-008: MBIE **should** establish a Business Connect Governance Group that has a formal mandate to review and approve changes to the platform.	38
Rec-009: MBIE **should** review and update the Business Connect Privacy Statement to ensure that it properly reflects the findings in this PIA, the ways in which MBIE will use Business Customer Profile Data, MBIE's status as processor and controller, and that it provides business customers with clarity on the status of Business Connect stakeholders.	39
Rec-010: MBIE **should** ensure that the benefits of permitting business customers to store documents on the Business Connect platform outweigh the privacy and security risks, and disable the feature if they do not.	41
Rec-011: MBIE **should** develop and implement a data retention policy and associated process for Business Customer Data, including submitted applications.	42
Rec-012: MBIE **must** develop and implement a data retention policy and associated process for Business Customer Profile Data and Platform Usage Data.	42
Rec-013: MBIE **should** develop a **Business Connect Data Protection and Use Policy** to set guardrails on access to, use of, and disclosure of data for the Business Connect team.	43
Rec-014: MBIE **could** consider developing a privacy training programme specific to Business Connect, to embed the Business Connect Data Protection and Use Policy.	43

Recommendation	Page
Rec-015: MBIE **could** develop and implement a **Business Connect Client Agency Privacy Checklist** to promote privacy compliance by GSPs.	44
Rec-016: MBIE **could** consider developing a **Business Connect Privacy Statement Generator**, as part of the components offered to GSPs via Business Connect.	45
Rec-017: MBIE **could** enable GSPs to add "tips" to forms to provide business customers with clarity about the collection of sensitive or unexpected personal information.	45

Glossary of terms

Term	Definition
Application and Case Data	All data about a specific application that has been submitted to the GSP, including application data and case workflow data.
Business Connect stakeholder	The stakeholders listed and explained in section 3.4, including the Host Agency, GSPs, business customers, Datacom, Pega Systems, and AWS.
Business customer	The business user of the Business Connect platform, who may create a Business Connect account, associate their account with a business, and use the platform to submit service applications.
Business Customer Data	The data a business customer uploads to Business Connect as part of a specific application, before it has been submitted to the relevant GSP.
Business Customer Profile Data	The data elements a business customer uses to create their Business Connect account, such as name, identity credentials, contact details, and NZBN data.
Platform Usage Data	Data relating to the way a business customer has used the platform, including cookie data, device data, and analytics.
GSP	Government Service Provider – any public sector agency that uses Business Connect to provide a service to a business customer. GSPs could be government departments or local government agencies. GSP may also be referred to as 'Client Agency'.
Host Agency	The agency that hosts the Business Connect platform and has the lead contractual relationship with Datacom, the primary service provider. The Host Agency is currently MBIE.
IPPs	Information Privacy Principles, set out in section 22 of the Privacy Act 2020.
MBIE	The Ministry of Business, Innovation & Employment. MBIE is the Host Agency for Business Connect, but may also be a GSP if it hosts its own services on the platform.
Personal information	Any information about an identifiable individual, including information generated from cookies where this is associated with an identifier such as name, NZBN or IP address. It does not include information about an incorporated entity.
PIA	Privacy Impact Assessment – a risk assessment used to help agencies identify and evaluate the potential privacy impact of a project, process, or change.

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 Our purpose and scope

This is an independent PIA on the Business Connect Platform. This PIA has three primary purposes. The first is to identify the privacy risks MBIE is responsible for and assess whether they have been adequately managed. The second is to identify the risks associated with using service providers, including cloud-based providers that might store or process personal information overseas, and assess whether these have been properly addressed in the complex contractual approach taken. The third is to identify how MBIE can develop Business Connect tools and functionality to better support GSPs to meet their own privacy obligations.

The PIA is intended to build trust with all Business Connect stakeholders, enabling the growth and evolution of the platform in a way that will meet the needs of GSPs and the business community while protecting and respecting the personal information processed through it.

In scope	Out of scope
• Privacy implications for MBIE as Host Agency in relation to delivering the Business Connect platform for GSPs. • Privacy implications of using service providers to deliver the Business Connect platform. • Potential opportunities the Business Connect platform offers for enabling privacy best practice by GSPs, as part of the overall service offering.	• Technical security risks created by Business Connect. 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 compliance by individual GSPs in relation to the services they deliver via Business Connect, other than where this is directly relevant to the Business Connect platform.

1.2 The information we have considered

We interviewed key project stakeholders, subject matter experts, and government and business users of Business Connect, with a view to understanding the project, the platform and the data flows that underpin them. We also reviewed key project documentation, including business cases, contracts, Business Connect collateral, and privacy and security risk

assessments already completed by MBIE. 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, summarised below. Throughout the PIA, recommendations are highlighted in yellow, and key observations are highlighted in green.

Regulatory context	This section will outline the relevant regulatory context within which this PIA is completed, including the Privacy Act and government Data Protection and Use Policy.
Project and platform	This section will outline Simply Privacy's understanding of Business Connect, from a technical, operational, and contractual perspective.
Personal information flows	This section will outline the data flows required to manage the Business Connect platform and the services it enables.
Summary of IPP application	This section will summarise the application of the Information Privacy Principles (**IPPs**) to Business Connect, 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 Business Connect. It is structured to reflect risks created by the use of service providers, risks to the Host Agency, and opportunities the Host Agency has to improve overall privacy compliance and people-centred service delivery.

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 MBIE, Datacom, and other stakeholders. 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. Regulatory context

This section outlines the relevant regulatory context within which this PIA is completed.

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 Business Connect stakeholders 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 that privacy risk must not be viewed in isolation. When assessing privacy risks and opportunities for Business Connect, we must consider the stakeholders' other legal and contractual obligations, their ability to deliver services efficiently and effectively, and the broader community benefits of improving business productivity.

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.

Further to this, 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.

[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), governance and 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.

DPUP has been designed to apply to the work of a wide range of public sector agencies with a role in ensuring public service outcomes, including agencies involved in funding, contracting, and partnering, the development of policies and programmes, and research and evaluation. Though not mandatory, agencies are encouraged to adopt DPUP in a way that makes sense for their work and their communities.

3. Project and platform

This section will outline Simply Privacy's understanding of Business Connect, from a technical, operational, and contractual perspective.

3.1 Business Connect purpose and vision

MBIE, through its Better for Business (B4B)[2] initiative, developed Business Connect in 2019 off the back of research which showed that businesses had a generally poor experience of dealing with government application processes, including:

- Repeatedly sharing the same information with different agencies, and even with the same agency
- Navigating government silos and trying to make sense of different but related regulations
- Limited transparency around the application processes, including stages and timing.

The purpose of Business Connect is to provide business and government with a common platform to enable government agencies to digitise and streamline business services and interactions across central and local government. The platform seeks to:

- Reduce the administrative cost involved for businesses to deal with government
- Increase business productivity and wellbeing, by enabling people to spend more time on their business and less time dealing with government
- Improve the transparency of, and trust in, government services, leading to improved compliance with regulatory requirements
- Enable government agencies to deliver more integrated front end digital services to businesses, at a lower cost
- Reduce duplication of effort in designing and delivering digital services
- Speed up processing times by reducing the manual handling of applications
- Improve data quality and regulatory compliance.

To deliver to its vision, MBIE has designed, and continues to evolve, Business Connect to meet the following key criteria:

- Be **accessible** – a multi-channel solution for businesses and agencies to apply for and process digital services

[2] B4B was established in 2012 as part of 'Better Public Services – Result 9'. It works across government to help reduce the cumulative administrative impact of compliance on business and to identify opportunities to improve the overall experience of dealing with government.

- Enable **reusability** of authoritative information across various service requests and all levels of government
- Drive **efficiency** – reduce time to complete a permission-based service request for a business customer and for a GSP to process a request
- Be **customer centric** – put the business customer experience at the heart of the service
- Provide **traceability and visibility** to the business customer in relation to the processing of service requests
- Provide **transparency** to business customers, so they have a holistic view of their service requests across government
- Provide GSPs with a **simpler, smarter** way to deliver and view services to businesses.

3.2 Business Connect today

Business Connect commenced in late-2019 with a pilot involving a limited set of local government services, including applications for food and beverage licenses. During the Covid-19 pandemic, Business Connect also supported businesses to obtain permission to travel across the Auckland alert level boundaries.

Since that time, the number of GSP services offered through the platform has steadily increased. The services now available on Business Connect include:

- Apply to MBIE for the fog canon subsidy scheme
- Apply to a local council for an Alcohol Licence
- Register a new food business with a local council
- Apply to Customs for a Deferred Payment Account
- Apply to Customs for participation in the Secure Exports Scheme
- Soon, business and individual users will also be able to apply to the Intellectual Property Office of NZ (**IPONZ**) for a NZ registered trademark.

The Business Connect Advisory Board is continuously working to increase government and business engagement with Business Connect, including promoting adoption of the platform by GSPs to support their services. MBIE expects the number of services supported by Business Connect to grow significantly in the coming years.

If a GSP wants to create a new service on Business Connect, the GSP will sign an MoU with MBIE as the Host Agency, and complete a scoping document, describing the service and associated requirements. Business Connect architects and analysts will then work with the GSP to design the service within the platform. This requires Business Connect to understand the data flows, integrations required, types of users, and other features of the service. The overall process includes an initial questionnaire, several information gathering sessions with the GSP, and prototyping sessions to ensure the service is fit for purpose.

Once the service is built and implemented on the Business Connect platform, GSPs can view and manage their cases on the platform. They can also choose how they want the Business Connect platform to integrate with their backend systems. This will depend on the maturity of the GSP and the specific requirements of the service.

- In some cases (such as for small local government agencies), the GSP might choose to host the entire service workflow on Business Connect.
- In other cases (and more often for larger government agencies), the GSP will use Business Connect as the frontend for their service, and will integrate the platform with their own backend systems via APIs, to allow them to process applications internally.

Business Connect user experiences and functions for both GSP users and business customers are outlined in more detail in section 4.

3.3 Business Connect tomorrow

To ensure that Business Connect continues to meet its vision and deliver to the key criteria set out at section 3.1, it is necessary to continue evolving the platform, with a focus on creating a generic Platform-as-a-Service product that will be of use to all GSPs, rather than bespoke services and functionalities for each GSP. While Business Connect will continue to provide analyst and expert support to GSPs to build and refine their services, the process will become quicker and simpler for all involved.

Business Connect is the fastest way to build great government services that businesses love[3]

MBIE is contemplating two specific future use cases for moving Business Connect to the next phase:

1. **Quick Forms**
   Business Connect analysts, on behalf of the GSP, will be able to quickly build services from a catalogue of form and function components. While this was initially intended to be a self-service option for GSPs, the Business Connect Advisory Board has determined that Business Connect should continue to provide GSPs with support to build their service. Services that used to take months to design and build will be developed and implemented in days.

2. **Case Management**
   Quick Forms is intended to be a "gateway" to the use of Business Connect's case management workflows, built with Pega's "out of the box" case management engine and functionality to manage an application from start to finish, and close it out within the platform. The benefits of this approach will include consistency of experience across all

[3] Business Connect's most recent vision.

services for GSP users, cost benefits as a result of economies of scale, and better integration between the frontend and backend of the services.

MBIE also recognises that it has an opportunity to provide GSPs with guidance and tools to better comply with privacy requirements. Put another way, implementing strong privacy tools and functionality within the platform for GSPs gives Business Connect an advantage. It can promote the platform as a way to better ensure that government services are privacy compliant and will maintain public and stakeholder trust. In view of growing consumer expectations about privacy, and privacy law reforms that will significantly increase risk, this will be an attractive proposition to most GSPs.

3.4 Shared services approach

Business Connect is currently delivered via a relatively complex 'shared services' approach to procuring, hosting and maintaining the platform. The approach enables a one-to-one contractual relationship between a Host Agency and the primary service provider, Datacom, and the delivery of platform-related services to each GSP via a Memorandum of Understanding and several other contractual documents. The Host Agency would enforce rights and obligations in the Datacom Agreement (for example in relation to the management of personal information) on behalf of the GSPs.

Figure 1 – The shared services approach

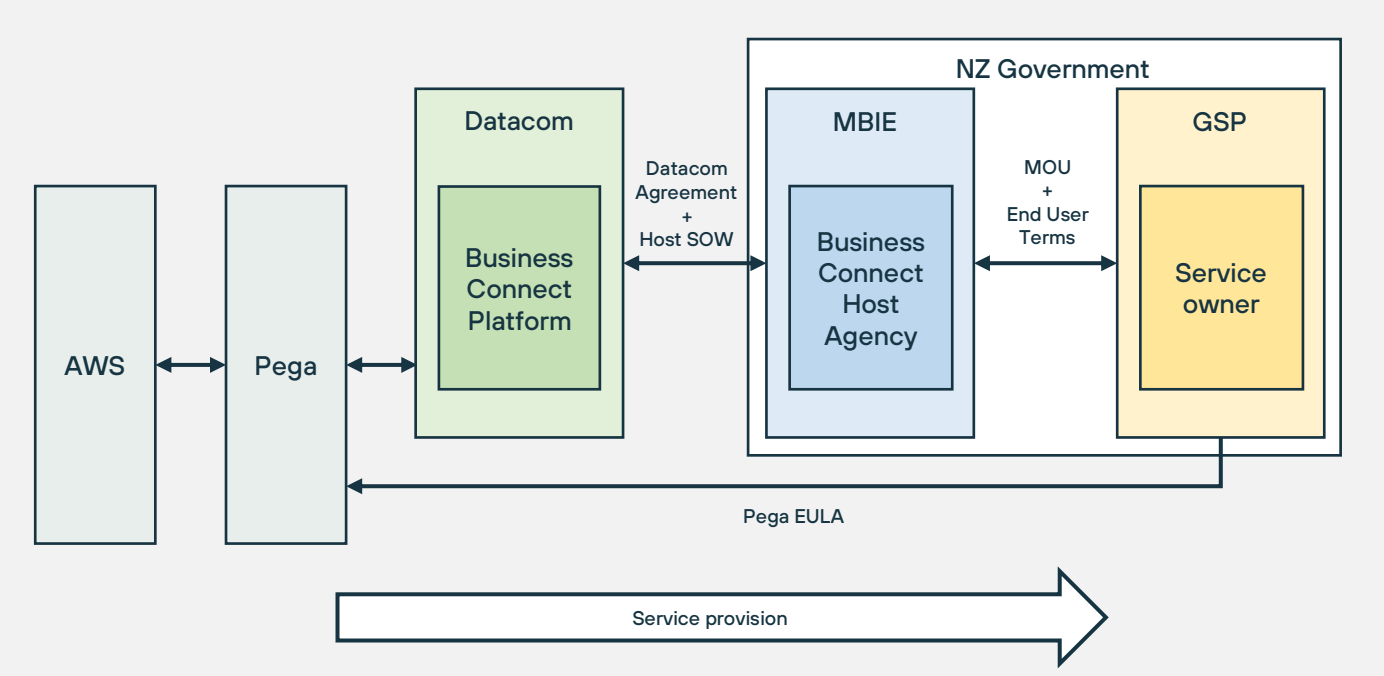


Figure 2 – Business Connect stakeholders

Stakeholder	Role
Host Agency	This is the agency that has the contractual relationship with the key Business Connect service provider, Datacom. Also referred to as the "lead agency", the Host Agency is responsible for contracting, hosting and maintaining the Business Connect service on behalf of the GSPs. It also assists GSPs to develop their services for use on Business Connect. The Host Agency is currently MBIE.
Government Service Provider (GSP)	This is the local or central government agency that owns the service being enabled via the Business Connect platform. Current GSPs include local councils and Customs. In the future, GSPs could include any central government agency that has services it needs to deliver to businesses or individuals via the platform.
Business customer	This is the person who uses the Business Connect platform to engage with GSP services. The business customer could represent an incorporated business or a sole trader, and a business customer might assign several staff to manage that business' Business Connect account. Current business customers include hospitality businesses (such as restaurants), and importers or exporters.
Datacom Systems Ltd (Datacom)	Datacom built, hosts and maintains the Business Connect platform on behalf of the Host Agency. Datacom provides a set of contracted support services, including platform maintenance, service desk, and service delivery management. It also generally collaborates with and supports the Host Agency to continually improve Business Connect.
Pega Systems	Business Connect is built on the Pega Platform. As such, Pega is a sub-processor to Datacom, providing the technology and functionality to deliver Business Connect. The Datacom Agreement includes as an appendix the End User Licence Agreement (**EULA**) for the Host Agency and GSPs to use Pega.
Amazon Web Services (AWS)	The data processed through the Pega Platform is stored in AWS data centres in Sydney. As such, AWS is a sub-processor to Pega.

3.5 Contractual framework

There is a complex set of contracts and agreements in place to manage Business Connect, reflecting the number of stakeholders involved and the various status of these stakeholders under the Privacy Act (privacy status is discussed further in section 3.6). The key contractual documents are summarised below and, where relevant, these are referenced in more detail in section 6.2.

- **Datacom Agreement**
  This is an agreement between MBIE (as the Host) and Datacom (as the Supplier) of Business Connect. As such, this is a critically important contract, which should clearly

establish controller (MBIE/GSP) and processor (Datacom) roles in relation to the personal information processed within Business Connect. The Datacom Agreement contains some privacy clauses, as between MBIE and Datacom, and also includes a Pega EULA (see below). The privacy clauses are discussed further in section 6.2.

- **Host Agency SoW**
  This is an agreement between MBIE and Datacom. The SoW records the terms on which Datacom must deliver support services to MBIE in relation to Business Connect. The SoW does not contain any clauses relating to privacy or data protection.

- **Host Agency - Client Agency MoU**
  This is a non-binding[4] agreement between the GSP and MBIE. The MoU is the most common way in which a GSP will engage with and use Business Connect. Under the MoU, MBIE manages the delivery of the new service to meet the GSP's requirements. The GSP is accountable for the delivery of the requirements, the security certification and accreditation of end-to-end workflow (excluding the Business Connect component) and managing interactions with the end user. Datacom is responsible for the provision of the resources under a SoW to develop the service and the support and performance of the platform along with the warranties they provide under the Datacom Agreement. The MoU links to the Datacom Agreement (see above) and the Client Agency End User Terms (see below).

- **Client Agency Agreement Template**
  This appears to be an agreement between the GSP and Datacom. However, this template has not generally been used by GSPs to engage with and use Business Connect, with the MoU summarised above being preferred. Accordingly, we have not reviewed this document.

- **Client Agency End User Terms**
  This is an agreement between the GSP and MBIE, which sets out the terms and conditions on which MBIE makes available Business Connect for use by the GSP. Linking back to the Datacom Agreement, the Terms better reflect the contractual realities of Business Connect than the MoU. Importantly, the Terms include privacy and data protection clauses that better ensure the GSP control over its own data. These are discussed further in section 6.2.

- **Pega End User Licence Agreement**
  This is an agreement between Datacom and Pega Systems. The EULA is intended to govern each GSP's use of the Pega Cloud Subscription Service, which underpins Business Connect. Because Pega, not Datacom, will manage most of the actual processing of personal information required to maintain Business Connect, this is an important document. The EULA includes significant privacy assurances, discussed further in section 6.2.

[4] Other than clause 15 which relates to confidentiality.

- **Business Terms of Use**
  This is an agreement between the business customer and MBIE. These Terms set out the terms and conditions on which business customers access and use Business Connect. The Terms link to a Business Connect Privacy Statement. The Terms and Privacy Statement are discussed further in section 6.3.2.

3.6 Privacy status of Business Connect stakeholders

The Privacy Act makes clear 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.[5] This distinction helps us to understand how privacy rights, responsibilities and liabilities attach to various agencies involved in a process. This, in turn, is a critical step in establishing how contracts, terms of use, and privacy statements should be drafted.

In summary, a controller determines how personal information should be collected, used and shared, and has the primary responsibility to ensure that the processing of personal information complies with the IPPs. The processor stores and processes personal information solely on behalf of the controller. This means it cannot process the information for its own purposes (if it does, it will cease being a processor). However, the flipside to this is that it has less responsibility to ensure compliance with the IPPs (with the exception of IPP 5 – security).

The status of Business Connect stakeholders is somewhat complex, and will depend on the nature of the services being delivered by each stakeholder, the type of personal information being processed, and the purposes of this processing.

Figure 3 – Status of Business Connect stakeholders

Data type	Controller	Processor
Business Customer Profile Data The data elements a business customer uses to create their Business Connect account, such as name, identity credentials, contact details, and NZBN data	**MBIE** MBIE, as the Host Agency, offers the Business Connect service to business customers regardless of which GSP they wish to interact with. MBIE has the primary relationship with the business customer in relation to their Business Connect account.	**Datacom/Pega/AWS**
Business Customer Data The data a business customer uploads to Business Connect as part of a specific application,	**Business Customer** This is on the basis that MBIE will not access or otherwise use the	**MBIE** **Datacom/Pega/AWS**

[5] 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.

Data type	Controller	Processor
before it has been submitted to the GSP	information, and so the business customer retains total control over it.	
Application and Case Data All data about a specific application that has been submitted to the GSP	**GSP** The GSP owns the service and determines what personal information needs to be collected and how it will be processed. The GSP has the primary relationship with the business customer in relation to the service.	**MBIE** **Datacom/Pega/AWS**
Platform Usage Data Data relating to the way a business customer has used the platform, including cookie data, device data, and analytics	**MBIE** MBIE, as the Host Agency, offers the Business Connect service to business customers regardless of which GSP they wish to interact with. MBIE has the primary relationship with the business customer in relation to general use of Business Connect.	**Datacom/Pega/AWS**

The upshot of this analysis is that:

- **GSPs** are responsible and liable *under the Privacy Act* for the collection and processing of personal information as part of a specific service being enabled on Business Connect (Application and Case Data).
- **MBIE** is responsible and liable *under the Privacy Act* for the collection and processing of personal information as part of setting up and maintaining business customer accounts and the platform generally (Business Customer Profile Data and Platform Usage Data).
- **MBIE** may be responsible and liable *under contract* for the collection and processing of personal information as part of a specific service being enabled on Business Connect, and has agreed in its contracts with GSPs to ensure Datacom manages Application and Case Data in accordance with the Privacy Act.
- **Business customer** is responsible and liable *under the Privacy Act* for the use of Business Connect to create and store Business Customer Data, though MBIE is responsible *under contract* for the storage and protection of this data.
- **Datacom, Pega and AWS** are responsible and liable *under contract* for the collection and processing of personal information in all contexts outlined above.

4. Personal information flows

This section will outline the data flows required to manage the Business Connect platform and the services it enables.

4.1 Personal information involved

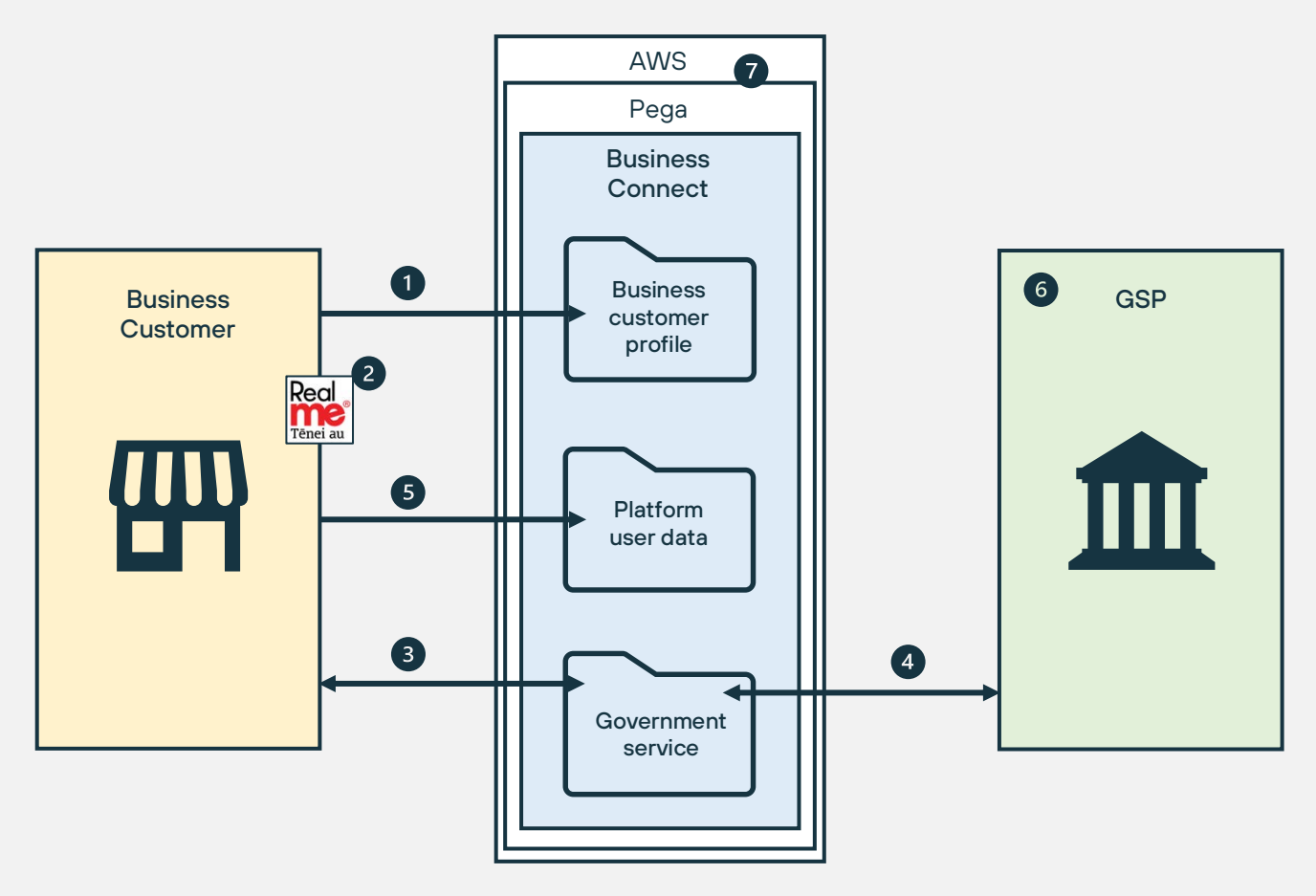
Figure 4 – Data elements collected or generated through Business Connect

Source	Information	Purpose	Comment
Business customer	Name	(MBIE) To create business customer user account	
	Contact details: - Phone number - Email	(MBIE) To create business customer user account, and receive notifications about applications	
	Information required for application	(GSP) To process and decide on application	Could include financial or other sensitive information
	Documents required for application	(GSP) To process and decide on application	Could include financial or other sensitive information
MBIE (NZBN)	NZBN public information: - Entity status - Entity name - NZBN - Entity type code - Entity type description - Source register - Source register ID - Address - Person role type (e.g. director) - Role status - Role start and end date	(MBIE) To create business customer user account (GSP) To process and decide on application	To connect a Business Connect account to a business, via the NZBN, the user must have authority over that business with NZBN, which then matches to Business Connect via RealMe
Generated by use of Business Connect	User device details, including: - IP address - Device type - Browser information	(MBIE) To understand user needs and optimise service and experience	

Source	Information	Purpose	Comment
	- Operating system - Country location - Preferred language		
	Platform usage data, including: - Search terms - Pages viewed - Date, time and duration of visit	(MBIE) To deliver platform functionality, improve functionality, improve security, and measure performance of the Platform	This information is generated by cookies, which business customers can disable in their browser (though this will affect the usability of the portal)

4.2 High-level data flows

Figure 5 – High-level data flows



1 Any person can create an account on Business Connect. To do so, the person must create a profile using their unverified RealMe identity, and will then use their RealMe

login to return to the Business Connect portal. To create an account, a person is required to provide their name, email address and phone number.

A user may also link their business to their Business Connect profile (this is required in relation to some services, such as Custom's Deferred Payment scheme). To do this, they must be listed with NZBN as having authority over that business. The system will ask them to verify their authority by logging into their NZBN account with the same RealMe profile they use to access Business Connect. The system will then ask for their permission to access information held about their business on the NZBN Register. If their RealMe profile matches an authority for a business listed in the NZBN Register, that business will be associated with their account.

2. Business Connect is integrated with RealMe to allow for trusted third-party identity management that can link with other government services using RealMe, such as the NZBN. As noted above, business customers will be required to use their personal RealMe accounts to log in to Business Connect and to associate their account with a business.

3. The business customer can then make service applications on behalf of the business, using the forms required by the relevant GSP for that service. The business customer can also upload documents in support of an application. Within the platform, the business customer can view all applications made, amend applications that have not yet been submitted and, in some cases, monitor the progress of their applications. Where an application has not yet been submitted, the GSP will not be able to view or access any information in that application.

4. The GSP can view all cases relating to applications for their services. If the GSP does not use Business Connect as a case management tool, the submissions will be provided to the GSP by email (as PDFs), or via an API into their own backend system of choice (such as SharePoint).

   If the GSP does use Business Connect as a case management tool, a GSP user will be able to view their own work queues, viewing and managing submissions that have been assigned to them. This could include any documents that have been uploaded in support of an application. From here, the GSP user can ask the business customer for more information, and can approve or decline the application.

   For the GSP Business Connect is case-based, not customer-based, which means a GSP user can never access a business customer's account profile. However, the GSP will be able to generate dashboards and other reports relating to the cases in their overall work queues.

5. As with most online platforms, Business Connect collects and uses Platform Usage Data (as outlined in Fig. 4 above) in order to understand user needs, optimise service and experience, deliver platform functionality, improve functionality, improve security, and measure performance of the platform. MBIE (via Datacom) uses Google Analytics and Hotjar for this purpose.

6 Whether the GSP uses Business Connect case management functionality or its own backend systems, it will be able to pull personal information related to service applications and retain this information in its own backend systems. This is appropriate, because the GSP is the controller for the purposes of this information. How the GSP manages this information once it is in its own backend systems is outside the scope of this PIA.

7 All data collected or generated within Business Connect is stored and processed by Pega Systems on the Pega Platform. The Pega Platform is hosted by AWS, and Business Connect data will be stored in AWS data centres in Sydney. Pega has committed to moving Business Connect data to data centres located in NZ once these are available. Datacom will also have access to Business Connect data in accordance with its rights and obligations under the Datacom Agreement.

Business Connect is not intended to be the system of record for GSP services, or the source of truth. It is a transactional platform only. For this reason, GSPs must ensure that they move any application data they need to retain to their own backend systems. Business Connect could be configured to delete data about submitted cases on request of the relevant GSP, though it never has been. Data about draft applications (which have not been submitted to the GSP) will be deleted after 6 months of no activity, after a warning email has been sent to the business customer.

5. Summary of IPP application

This section will summarise the application of the IPPs to Business Connect, with a view to identifying areas of risk and opportunity that should be given more detailed consideration in section 6. It should be noted that risks, and solutions, can impact several IPPs simultaneously.

<table>
<tr><th>IPP</th><th colspan="2">Considerations</th></tr>
<tr><td rowspan="2">1. Collect only personal information that is necessary for a lawful purpose</td><td colspan="2">For GSP

The GSP must ensure that it collects only the personal information it needs to manage a specific service via Business Connect. This includes minimising the required fields to be completed within an application form and minimising the scope of documents a business customer is required to submit in support of an application.</td></tr>
<tr><td>For Host Agency as processor

This obligation rests solely on the GSP, in relation to Application and Case Data. Compliance with IPP 1 will depend on the requirements for the particular service. However, MBIE can assist GSPs to comply with IPP 1, by designing Business Connect service development processes to enable data minimisation.

See section 6.4.1</td><td>For Host Agency as controller

MBIE must ensure that it collects only the personal information it needs for the purposes of managing business customer accounts and platform usage (including web analytics). The data collected is set out above at section 4.1. There is no evidence that MBIE is currently collecting more information than it needs for these purposes. At this point, MBIE is complying with IPP 1.</td></tr>
<tr><td>2. Collect personal information directly from the person concerned</td><td colspan="2">For GSP

The GSP must ensure that it collects personal information directly from the business customer, unless it has a lawful basis to collect information from a third party. All the information the GSP collects as part of a service application will be collected directly from the business customer via the application process. This complies with IPP 2.</td></tr>
</table>

IPP	Considerations	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to Application and Case Data.	*For Host Agency as controller* Business Connect integrates with some third-party sources as part of the business customer account set up process, including NZBN. This information is generally pulled into Business Connect with the express consent of the business customer, and so is permitted by IPP 2(2)(c).
3. Tell people why personal information is required, how it will be used, and who it may be shared with	*For GSP* The GSP must ensure that it is transparent with business customers about the personal information it collects for the purpose of a service. This includes ensuring that the business customer is aware which agency is collecting the information. At present, specific services within Business Connect are clearly branded according to the relevant GSP. This means it is clear to the business customer which agency is collecting their information. However, the services reviewed for this PIA included no specific privacy notices for the services, or links to the GSP's general privacy statements. At present, therefore, the requirements of IPP 3 are not consistently being met.	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to Application and Case Data. However, MBIE can assist GSPs to comply with IPP 3, by designing Business Connect service development processes to enable GSPs to deliver transparency. See section 6.4.1	*For Host Agency as controller* MBIE must ensure that it is transparent with business customers about the personal information it collects for the purposes of managing business customer accounts and platform usage. MBIE has developed a Business Connect Privacy Statement, which is made available to business customers on the portal. The statement is simple and clear, and provides good notice in relation to web analytics and account data. However, the statement could be improved to ensure business customers understand the controller/processor distinction in relation to GSP services. See section 6.3.2

IPP	Considerations	
4. Collect personal information in ways that are lawful, fair, and not unreasonably intrusive	*For GSP* The GSP must ensure that it collects Application and Case Data in a manner that is lawful, fair, and not unreasonably intrusive. This requires consideration of necessity and proportionality. For the most part, the services delivered via Business Connect will not raise fairness or intrusiveness issues, but this does rely on GSPs properly meeting their data minimisation and transparency requirements.	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to Application and Case Data.	*For Host Agency as controller* MBIE must ensure that it collects Business Customer Profile Data and Platform Usage Data in a manner that is lawful, fair, and not unreasonably intrusive. The only collection of information that might raise intrusiveness issues for MBIE is the collection of web analytics data, particularly via the use of cookies. However, MBIE has taken steps to ensure transparency in relation to this collection, and business customers do have the option to disable cookies in their web browsers. Further, the web analytics MBIE is undertaking appear to be industry standard and would be unlikely to come as a surprise to business customers.
5. Take reasonable steps to keep personal information safe and secure	*For GSP* The GSP must ensure that Application and Case Data is secure. Because the GSP is the controller in relation to this information, this obligation covers the entire end-to-end process for a service, and extends to ensuring that its processors – MBIE, Datacom, Pega and AWS also keep the information secure. While the MoU states that the GSP is not responsible for ensuring security in relation to the Business Connect platform itself, that is a contractual exclusion only – the GSP is jointly liable for the platform under the Privacy Act, at least in relation to the storage and processing of Application and Case Data on it.	

IPP	Considerations	
	For Host Agency as processor As a processor, and as the lead government agency in respect of the Business Connect Platform, MBIE must take steps to assist GSPs to meet their obligations under IPP 5. This includes ensuring that the other processors – Datacom, Pega and AWS – are able and willing to meet their contractual obligations to keep personal information secure while it is in their control. See section 6.2 and section 6.3.3	*For Host Agency as controller* MBIE must ensure that Business Customer Profile Data and Platform Usage Data is secure. The risk here is somewhat lower, as this data is not sensitive. On this basis, the security measures already in place to ensure Business Connect is secure are more than adequate for the purposes of protecting this data. See section 6.2 and section 6.3.3
6. Let people access their information	*For GSP* The GSP must ensure that business customers can access their information when they request it. This will generally be enabled by the Business Connect platform itself, which allows business customers to access their profiles, draft or submitted applications, or documents directly via the user portal. On this basis, the use of Business Connect by GSPs is likely to improve compliance with IPP 6.	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to Application and Case Data. However, as noted above, MBIE assists GSPs to comply with IPP 6 by providing business customers with direct access to their information. See section 6.4.3	*For Host Agency as controller* As noted above, business customers can access their profiles, draft or submitted applications, or documents directly via the user portal.
7. Let people correct their information	*For GSP* The GSP must ensure that business customers can request to correct their information. Business customers will be able to access and correct their profiles and draft applications directly via the user portal. However, once an application has been	

<table>
<tr><th>IPP</th><th colspan="2">Considerations</th></tr>
<tr><td></td><td colspan="2">submitted, it will not be possible for a business customer to correct it via the portal. Therefore, GSPs will need to ensure that they have internal processes in place to enable the correction of applications once submitted.</td></tr>
<tr><td></td><td>For Host Agency as processor

This obligation rests solely on the GSP, in relation to Application and Case Data. However, as noted above, MBIE assists GSPs to comply with IPP 7 by providing business customers with the ability to correct their information.

See section 6.4.3</td><td>For Host Agency as controller

As noted above, business customers can access and correct their profiles and draft applications directly via the user portal.</td></tr>
<tr><td>8. Take reasonable steps to check personal information is accurate before using it</td><td colspan="2">For GSP

The GSP must ensure that Application and Case Data is accurate, up to date, and complete before using it to decide on the application. For the most part, accuracy is managed by the business customer directly, as part of the process of providing the information via the Business Connect portal. The GSP can use Business Connect to engage with a business customer and request more, or updated, information as part of the application process. Business Connect also automates the process of connecting a business customer to the correct business, via RealMe and NZBN.</td></tr>
<tr><td></td><td>For Host Agency as processor

This obligation rests solely on the GSP, in relation to Application and Case Data. However, as noted above, MBIE assists GSPs to comply with IPP 8 by allowing business customers to link their businesses by verifying their NZBN authority, and by providing business customers an easy way to update documentation where required by the GSP.</td><td>For Host Agency as controller

Data accuracy is a lower risk in relation to Business Customer Profile Data and Platform Usage Data. It is enough, in this case, that a business customer can access and update their account details directly via the user portal.</td></tr>
</table>

<table>
<tr><th>IPP</th><th colspan="2">Considerations</th></tr>
<tr><td>9. Don't retain personal information for longer that it's needed for a lawful purpose</td><td colspan="2">For GSP

The GSP must ensure that it does not retain Application and Case Data in its backend systems for longer than it has a lawful purpose to use it. For GSPs, this will involve a consideration of any minimum data retention requirements set by relevant laws or regulations (including the Public Records Act or relevant General Disposal Authorities), and maximum data retention requirements set by its legitimate use of the information for the purposes of the service.</td></tr>
<tr><td></td><td>For Host Agency as processor

This obligation rests solely on the GSP, in relation to the retention of Application and Case Data within GSP backend systems.

However, MBIE should enable business customers to determine how long their submitted applications are retained within the Business Connect portal. MBIE currently intends to delete draft applications after 6 months of no activity (following a warning to the business customer). This is not about compliance with IPP 9 but rather to ensure that a draft application is not corrupted by form changes related to that specific application.

See section 6.4.4</td><td>For Host Agency as controller

MBIE must ensure that it does not retain Business Customer Profile Data and Platform Usage Data for longer than it has a lawful purpose to use it.

See section 6.3.4</td></tr>
<tr><td>10. Use personal information only for the purposes it was collected</td><td colspan="2">For GSP

The GSP must ensure that it uses Application and Case Data only for the purpose of deciding on a service application, or in other ways as notified to business customers in its privacy statement.</td></tr>
</table>

IPP	Considerations	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to the use of Application and Case Data. However, as a processor, MBIE must ensure that it does not access or use Business Customer Data or Application and Case Data for any purpose other than delivering the services to business customers and GSPs. If it does, it will become a controller in relation to that information, and subject to the full force of the Privacy Act. See section 6.3.5 and 6.4.5	*For Host Agency as controller* MBIE must ensure that it uses Business Customer Profile Data and Platform Usage Data only for the purposes it was collected, and only in the ways it has notified to business customers in the Business Connect Privacy Statement. See section 6.3.5
11. Don't disclose personal information, unless an exception applies	*For GSP* The GSP must ensure that it does not disclose Application and Case Data, unless that disclosure is directly related to the processing of that application, or has been otherwise notified to business customers in its privacy statement. It should be noted that using MBIE (as Host Agency), and Datacom, Pega and AWS as sub-processors, to deliver Business Connect services (including workflow services) does not constitute a "disclosure" by the GSP for the purposes of IPP 11, because MBIE is processing this information solely on behalf of the GSP (see section 11 of the Privacy Act).	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to the disclosure of Application and Case Data. However, as a processor, MBIE must ensure that it does not disclose Business Customer Data or Application and Case Data for any purpose other than delivering the services to business customers and GSPs. If it does, it will	*For Host Agency as controller* MBIE must ensure that it does not disclose Business Customer Profile Data and Platform Usage Data, unless that disclosure is directly related to the purposes for which the data was collected, and has been notified to business customers in the Business Connect Privacy Statement. It should be noted that sharing personal information with Datacom, Pega, AWS, Google Analytics, and Hotjar does not constitute a

IPP	Considerations	
	become a controller in relation to that information, and subject to the full force of the Privacy Act. It should be noted that passing personal information to the relevant GSP as part of the Business Connect service does not constitute a "disclosure" by MBIE for the purposes of IPP 11, because MBIE is processing this information on behalf of the business customer, who chooses to disclose the information to the GSP when clicking 'submit'. Once the application has been submitted, any new information about the submitted application created within Business Connect is deemed to be held by the GSP. See section 6.3.5 and 6.4.5	"disclosure" for the purposes of IPP 11 because these agencies are processing the information solely on MBIE's behalf. See section 6.3.5
12. Only disclose personal information to overseas third parties if it is subject to comparable privacy safeguards	*For GSP* The GSP must ensure that does not disclose personal information collected for the purpose of a service to an overseas recipient, unless it has reasonable grounds to believe that the information will be protected to a standard comparable to that required by the Privacy Act. This is unlikely to occur in relation to most GSP services. It should be noted that overseas processing of personal information on the Pega Platform, or storing personal information in AWS data centres overseas, does not engage IPP 12, because this does not constitute a "disclosure" for the purposes of IPP 11.	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to the disclosure of Application and Case Data. It should be noted that overseas processing of personal information on the Pega Platform, or storing personal information in AWS data centres overseas, does not	*For Host Agency as controller* MBIE must ensure that it does not disclose Business Customer Profile Data and Platform Usage Data to an overseas recipient, unless it has reasonable grounds to believe that the information will be protected to a standard comparable to that required by the

IPP	Considerations	
	engage IPP 12, because this does not constitute a "disclosure" for the purposes of IPP 11.	Privacy Act. This is unlikely to occur in relation to Business Connect. It should be noted that sharing personal information with Pega, AWS, Google Analytics, and Hotjar – which may store or process that information overseas – does not engage IPP 12, because this does not constitute 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	*For GSP* The GSP must ensure that it collects and uses unique identifiers for service application purposes in accordance with the requirements of IPP 13. In the Business Connect context, the key identifier used is the NZBN. Where a business is unincorporated – for example a sole trader – the NZBN is a unique identifier for the purposes of IPP 13, as it uniquely identifies that sole trader. However, the collection and use of the NZBN by GSPs for the purposes of processing a service application is contemplated by the NZBN Act and so would be permitted by IPP 13.	
	For Host Agency as processor This obligation rests solely on the GSP, in relation to the collection and use of unique identifiers as part of its own service processes. However, as a processor, MBIE can assist GSPs to comply with IPP 13, including by protecting the NZBN from misuse while it is stored and processed within Business Connect, and by ensuring through robust process (including RealMe) that the correct NZBN is associated with the correct business customer.	*For Host Agency as controller* MBIE collects and uses the NZBN as part of the business customer account process. As noted above, this is permitted by IPP 13, as it is one of the purposes for which the NZBN has been assigned. As noted to the left, MBIE already has reasonable processes in place to ensure that the NZBN is only assigned to a business customer whose identity is clearly established (using RealMe), and that the NZBN is protected from misuse.

6. Privacy risk and opportunity assessment

This section will assess in more depth the key privacy risks and opportunities identified in section 5.

6.1 Overall privacy risk profile

Both Business Connect and the government services it facilitates are targeted at businesses, not individuals. This means that, for the most part, the information collected via Business Connect will be about incorporated businesses, and therefore not subject to the Privacy Act. On this basis alone, the privacy risk profile might be considered nominal.

However, there will be several scenarios – summarised below – in which Business Connect, and the GSPs using it, will be collecting personal information that is subject to the Privacy Act. This will elevate the overall privacy risk profile for Business Connect, and the findings and recommendations made later in the PIA reflect this.

Figure 6 – Scenarios in which personal information may be collected and processed by Business Connect or GSPs

	Where a business customer is a sole trader, most or all of the information provided by that customer to the GSP as part of a service will be personal information about them, because in the case of sole traders, information about their business is also information about them personally (for example, information about business revenue is essentially information about the sole trader's salary. Likewise, information about business debt or credit risk is essentially information about the sole trader's personal debt or credit risk).
	Where a business representative sets up a profile with Business Connect in order to use the platform, most of the details they submit, including their name and contact details, are likely to be personal information about them (though this information is not particularly sensitive).
Real me® Tēnei au	Business customers are required to use their personal RealMe accounts to verify their identity as part of the platform, and this RealMe information relates directly to them, not to the businesses they are representing.
	The collection of Platform Usage Data by Business Connect may involve the collection of personal information about the relevant business customer. For example, if the business customer is accessing Business Connect from their personal device, the device details collected (including IP address, location information etc) may be personal information about them.

Future services, such as the upcoming registration of trademarks with IPONZ, may be targeted at individuals (or consumers) as well as businesses. In these cases, all the information collected from the individual will be personal information.

6.2 Managing service provider risk

MBIE, as the Host Agency, has procured the services of several third-party service providers to deliver the Business Connect platform. As such, MBIE and the GSPs are entrusting data – including personal information – to these service providers, but remain liable for that data while it is in their care. As noted above, in some cases, MBIE is also acting as a service provider for the GSPs. 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.

6.2.1 Contractual assurances from Business Connect service providers

We have reviewed all the relevant contractual agreements relating to Business Connect, including agreements between GSPs, MBIE, and the service providers. These agreements are outlined in section 3.5. In addition, we have reviewed the universal Service Terms provided by AWS. These Service Terms apply to all services AWS offers, including cloud storage services.

In this review, we are assessing how well each contractual document reflects the status of the parties under the Privacy Act (as controller or processor), 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.

Figure 7 – High-level review of Business Connect contractual agreements

Assurance	MBIE[6]	Datacom[7]	Pega[8]	AWS[9]
1. The controller/processor distinction is recognised.	Yes – clause 9 of EUT	Yes – clause 17.4 - clause 17.5	Yes – clause 1(c)	Yes – clause 1.1 of DPA
2. The processor will use the information only to deliver the services or on the instructions of the controller, unless required by law.	Yes – clause 10(a) of EUT	Yes – clause 17.4(b) (Business Customer Data) - clause 17.5(a) (Client Agency Data)	Yes – clause 3(b)	Yes – clause 2 of DPA

[6] Combination of Host Agency-Client Agency MoU and Client Agency End User Terms.
[7] Datacom Agreement.
[8] Pega Platform End User Licence Agreement.
[9] AWS Service Terms and Data Processing Addendum.

Assurance	MBIE[6]	Datacom[7]	Pega[8]	AWS[9]
		- clause 17.6(a) (all data)		
3. The processor will protect the information with adequate organisational and technical security measures.	Yes – clause 10(c) of EUT - clause 10(e) of EUT	Yes – clause 17.6(e) - clause 17.6(f)	Yes – clause 4	Yes – clause 5 of DPA
4. The processor will not disclose the information to a third party, unless authorised by the controller or required by law.	Yes – clause 10(b) of EUT - clause 12 of EUT	Yes – clause 17.6(b) - clause 17.7	Yes – clause 8	Yes – clause 3 of DPA
5. The processor will return and destroy the information on request from the controller or at the conclusion of the services.	No*	Yes - clause 28.5(b)(iv)	No^	Yes – clause 1.14.5 of Service Terms - clause 14 of DPA
6. The processor will notify the customer immediately of any privacy or data breach that affects the controller's information.	No* - clause 10(f) of EUT does not mention notification	Yes – clause 17.3	Yes – clause 7	Yes - clause 9 of DPA

6.2.2 Specific feedback on contractual arrangements

Subject to the recommendations below, the combination of contractual documents, while complex, should deliver an effective "chain of command" that will ensure GSPs and MBIE can maintain control of the personal information that is being processed on their behalf by the sequence of service providers involved.

This is on the basis that:

- Clause 4(d) of the Host Agency-Client Agency MoU states that MBIE will "ensure Datacom handle any Agency information in accordance with the information handling requirements set out in the Datacom Agreement" (see column three above).
- Clause 10 of the Client Agency End User Terms states that MBIE will meet its privacy and security obligations via its contract terms with Datacom (see column three above).

- Clause 10(e) of the Client Agency End User Terms states that MBIE will "ensure Datacom complies with the security requirements in the New Zealand Information Security Manual (NZISM) in helping provide Business Connect".
- The Pega Platform EULA, which is appended to the Datacom Agreement, is intended to protect each GSP's data and is enforceable via Datacom as the Supplier (see column 4 above).
- AWS provides industry standard privacy and security assurances as part of its Universal Service Terms and Data Processing Addendum. These assurances are enforceable by the GSPs and MBIE via the Pega EULA.

However, some improvements could be made to several of the contractual documents to ensure that there is clarity in respect of important data rights and responsibilities.

*Client Agency End User Terms

- The End User Terms do not specifically address the deletion of Application and Case Data on termination. Because business customers use Business Connect for the purposes of maintaining a record of their applications for services, this may be appropriate. However, as discussed below at section 6.3, MBIE will need to consider whether business customers should have the ability to delete their submitted applications from the platform.

- The End User Terms do not specifically address the notification of privacy breaches to GSPs. However, because MBIE essentially meets its privacy and security obligations in respect of Business Connect via Datacom, this is appropriate. Both the Datacom Agreement and the Pega EULA contain appropriate and sufficient privacy breach notification assurances, that should ensure GSPs are notified in the right circumstances.

- Clause 10(f) of the End User Terms states that MBIE will "remedy and manage any privacy breach as soon as it becomes aware of the breach". However, there is no clarity here as to which party to the agreement – MBIE or the GSP – should manage the notification of privacy breaches to the Privacy Commissioner or affected business customers. This should be expressly addressed in the End User Terms to avoid confusion or duplication of effort in the event of a breach.

Rec-001: MBIE **should** Amend the Client Agency End User Terms to expressly provide for the notification of privacy breaches to the Privacy Commissioner or affected business customers and ensure that the parties are clear as to which agency will manage this decision and process.

Datacom Agreement

- "Client Agency" is defined in clause 1.1 of the Datacom Agreement as an agency that has entered into a Client Agency Agreement using the Client Agency Agreement Template. However, as noted above at section 3.5, it is our understating that GSPs rarely enter into Client Agency Agreements, preferring the combination of MoU and Client Agency End

User Terms. This issue may impact on the effectiveness of the assurances provided in the Datacom Agreement and Pega EULA, as GSPs may not meet the definition of Client Agency.

Rec-002: MBIE **should** consider whether the definition of "Client Agency" in the Datacom Agreement needs to be amended to reflect actual practice.

- Datacom provides data processing services to MBIE as Host Agency as well as to GSPs. As noted above, MBIE is the controller in relation to Business Customer Profile Data and Platform Usage Data. However, the definition of "Client Agency Data" – which is protected under the Datacom Agreement – does not appear to include personal information processed and stored on behalf of the Host Agency. This could leave MBIE exposed in respect of the personal information it is directly responsible for.

Rec-003: MBIE **should** consider whether the definition of "Client Agency Data" in the Datacom Agreement should be amended to include information being processed on behalf of the Host Agency in its role as controller.

- Clause 17.3 of the Datacom Agreement relates to the notification (described as "escalation") of privacy breaches to the Host Agency and affected GSP. This is positive. However, it is not clear from clause 17.3 which agency should manage the notification of privacy breaches to the Privacy Commissioner or affected business customers. It is important that breach notification decisions are not managed by Datacom or any other service provider, but rather by the Host Agency or GSP (see above).

Rec-004: MBIE **should** amend clause 17.3 of the Datacom Agreement to make clear that any decision to notify the Privacy Commissioner or an affected business customer of a privacy breach must be made by either the Host Agency or affected Client Agency, not by Datacom or any other service provider.

^Pega EULA

- The Pega EULA does not specifically address the deletion of Business Connect data on termination (either by the GSP, MBIE or Datacom). Clause 9(d) (which relates to term) places an obligation on GSPs to return any Pega confidential information on termination. However, there appears to be no such obligation on Pega to return or destroy Business Connect data on termination. While the Datacom Agreement places such an obligation on Datacom, this may not be enough to ensure that Pega is not permitted to retain copies of the data outside the Business Connect instance of the Pega Platform.

Rec-005: MBIE **should** request that Pega amend the Pega EULA to include a clause relating to the return and/or destruction of Business Connect data on termination of the services.

Business Connect Product Overview

In addition to the contractual documents discussed above, MBIE has developed the Business Connect Product Overview, which is referenced in the Client Agency End User Terms. The Product Overview includes privacy and security responsibilities on both MBIE and the GSP, each of which commits to comply with these responsibilities in the End User Terms.

This document provides useful, and often detailed, information to GSPs about how security is managed for Business Connect. However, the section entitled "**It's data is private**" could be redrafted to better reflect the findings in this PIA, and provide more clarity around the status of all stakeholders under the Privacy Act (and how this translates into service design and operation).

Rec-006: MBIE **could** update the Business Connect Product Overview to reflect the findings of this PIA and provide better clarity to GSPs on the roles and responsibilities of all stakeholders under the Privacy Act.

6.2.3 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, Business Connect data will be stored at rest in **Australia**.[10] Australia has a privacy framework in place that is more robust than NZ. 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, and the type of data being processed on Business Connect, the likelihood of Australian Government agencies seeking access to Business Connect data stored in Australian-based servers is low. On this basis, the jurisdictional risk for Australia is acceptable.[11]

[10] Note, clause 5 of the Pega EULA states that Pega must not transfer Business Connect data outisde New Zealand or Australia without the written consent of the relevant GSP.
[11] 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

AWS intends to build new data centres in NZ,[12] which will allow the company to establish a NZ AWS region. Datacom has advised that Pega has made a commitment to move its NZ clients to the NZ AWS region once this is available. This is recommended, as it would significantly reduce jurisdictional risk and address other concerns including in relation Māori data sovereignty.

Rec-007: MBIE **should** consider moving Business Connect data at rest to AWS data centres within the NZ AWS region when this option is available.

6.3 Privacy risks for Host Agency

This section outlines privacy risks specific to MBIE as the Host Agency. They relate to MBIE's role as processor of Application and Case Data and Business Customer Data, and to MBIE's role as controller of Business Customer Profile Data and Platform Usage Data.

6.3.1 Governance to ensure Privacy by Design

As Business Connect continues to evolve and grow, MBIE must ensure that the platform retains its privacy and security settings and remains the safest option for GSPs. This will require a robust governance and accountability framework and change management process to ensure that privacy risk is always considered as part of product and service development.

Currently, there is no governance group for Business Connect. The existing Business Connect Advisory Board has a mandate to increase government and business engagement with Business Connect, but no formal oversight of the development or operation of Business Connect. This leaves MBIE significantly exposed to risk.

MBIE should establish a Business Connect Governance Group (which must include senior MBIE representatives, and could also include GSP representatives) that has a formal mandate to review and approve changes to the platform, to ensure that they:

- incorporate the principles of Privacy by Design, including ensuring end-to-end security, user-centricity and privacy settings by default;
- do not prejudice GSP compliance with the Privacy Act; and
- reflect and respect the privacy status (processor or controller) of each Business Connect stakeholder.

Rec-008: MBIE **should** establish a Business Connect Governance Group that has a formal mandate to review and approve changes to the platform.

this function, the Service must maintain parliamentary privilege and consider national security implications of exposing parliamentary communications to jurisdictional risk.

[12] https://www.nzherald.co.nz/business/infrastructure-data-cloud-centres-with-golden-lining/M6YWTF5JSBDITKKVRQCFDAL5OI/.

6.3.2 Privacy transparency for Business Connect users

Business customers will be required to engage with several different data controllers when using Business Connect – MBIE and the various GSPs they apply to for services. It is critically important that business customers are clear at all times about which controller they are dealing with in respect of the various processes required to use Business Connect.

GSPs are responsible for privacy transparency in respect of the specific services, and this is discussed further in section 6.4.2. MBIE is responsible for privacy transparency in respect of the collection and use of Business Customer Profile Data and Platform Usage Data. It should also, as a responsible Host Agency, provide additional privacy transparency to business customers in respect of the overall Business Connect platform and the role each stakeholder plays in the Business Connect ecosystem.

MBIE has developed a Business Connect Privacy Statement which delivers essential privacy notices to business customers. MBIE also provides business customers with Terms of Use that include reference to the Privacy Statement. These documents make a good start at ensuring clear privacy transparency, but the following observations are made:

- The Privacy Statement refers to the Privacy Act 1993, and should be reviewed and updated as against the Privacy Act 2020.
- The Privacy Statement provides no clear explanation of the complex platform arrangements in place, including MBIE's role as Host Agency and the role of various GSPs as data controllers.
- While the Privacy Statement does address the collection and use of Platform Usage Data, it provides no clarity on the ways MBIE (as data controller) may use Business Customer Profile Data.
- The Privacy Statement could provide more clarity to business customers in respect of their ownership of Business Customer Data that they upload to the platform, and their rights in relation to it.
- The access and correction sections of the Privacy Statement could better reflect the controller/processor distinction and provide more clarity about how these rights will be managed in practice (that is, via the platform in some cases, and by request to the relevant GSP in others).
- Clause 3.4 of the Terms of Use contain a good explanation of the RealMe integration, but this information might be better placed in the Privacy Statement. At a minimum, it would be worth repeating this content in the Privacy Statement.
- Clause 10.3 of the Terms of Use state that once data is transmitted to the relevant GSP, it is subject to that GSP's Privacy Statement. This is correct but, again, this content should be in the Privacy Statement.

Rec-009: MBIE **should** review and update the Business Connect Privacy Statement to ensure that it properly reflects the findings in this PIA, the ways in which MBIE will use Business

Customer Profile Data, MBIE's status as processor and controller, and that it provides business customers with clarity on the status of Business Connect stakeholders.

6.3.3 Platform security risks

Security is a critically important risk to manage in the context of a Platform-as-a-Service offering. Business Connect will only succeed if business customers and GSPs have full trust and confidence that the personal information (and sensitive commercial information) they process through the platform is safe and secure at all times. A significant security breach or failure could be fatal for the platform.

As with any cloud-based platform that incorporates layers of processors and sub-processors, the Business Connect platform is protected by a shared responsibility model. Under this model, processors have responsibility for the technical security measures in relation to their layers of the overall ecosystem, and controllers have a responsibility to ensure that organisational security measures are in place to complement these technical measures. For example:

- AWS will (and is required by contract to) ensure technical security measures are in place and operational in respect of their data centres and platforms;[13]
- Pega will (and is required by contract to) ensure technical security measures are in place and operational in respect of the Pega Platform;[14]
- Datacom will (and is required by contract to) ensure that Pega and (by extension) AWS meet their security obligations as noted above;
- MBIE (via Datacom) will ensure that organisational security measures, such as role-based access controls, are established and maintained;
- MBIE (as Host Agency) has an overall role in assessing and ensuring that all layers of the ecosystem are appropriately safe and secure; and
- Each GSP must be satisfied that the Business Connect platform meets government information security standards, and is appropriate for their use.

This is not a security assessment. However, as part of the overall PIA process, we have reviewed the relevant security documentation and interviewed IT Security staff. On the basis of this information, MBIE would appear to be taking reasonable steps to ensure that platform security risks are appropriately managed and mitigated.

These steps include obtaining third-party security risk assessments on the platform, completing and maintaining System Security Certificates (on a two-year certification and accreditation cycle) and completing security control reviews and remediation exercises. The primary security

[13] More information about AWS' technical and other security measures can be found at https://aws.amazon.com/compliance/data-protection/.
[14] More information about Pega's technical and other security measures can be found at https://docs.pega.com/en-US/bundle/pega-cloud/page/pega-cloud/pc/pcs-security-and-data-protection.html.

settings and measures are outlined in the Business Connect Certification and Accreditation Summary (November 2022).

There is, however, one specific security issue that was identified during the information gathering phase for this PIA:

- **Document storage service increases risk**
  A business customer can use Business Connect to store documents relevant to the service applications they may wish to make, for example in case they need to re-use these documents. Documents might include sensitive personal or commercial information. While this functionality will undoubtedly be of use to business customers, it will increase the privacy and security risk MBIE must manage as the Host Agency.

Rec-010: MBIE **should** ensure that the benefits of permitting business customers to store documents on the Business Connect platform outweigh the privacy and security risks, and disable the feature if they do not.

6.3.4 Data retention rules

MBIE will need to put rules in place to manage the retention of Business Customer Data (on behalf of business customers), Business Customer Profile Data and Platform Usage Data. Retention obligations in relation to Application and Case Data rest on the GSP and are discussed in section 6.4.4.

Business Customer Data (including submitted applications)

Noting that Business Connect is not intended to be the system of record for GSPs, business customers should have the ability to decide how long their draft and submitted applications (and associated documents) are retained within Business Connect. Ideally, this should be enabled by allowing business customers to delete documents, draft applications and submitted applications themselves. If necessary, a minimum retention period could be applied (for example 6 months) before a business customer can delete submitted cases. A maximum retention period that is prompted by a period of inactivity could also be applied to reduce the risk of indefinite retention by default.

Figure 8 – Sample data retention policy for Business Customer Data, including submitted applications

Information	Minimum retention period	Maximum retention period	Disposal action
Draft applications	None – may be deleted by business customer at any time	6 months after last action by business customer	Contact business customer, then delete

Information	Minimum retention period	Maximum retention period	Disposal action
Submitted applications	6 months, after which time business customer may delete	5 years after last action by business customer	Contact business customer, then delete
Documents	None – may be deleted by business customer at any time	5 years after last action by business customer	Contact business customer, then delete

Rec-011: MBIE **should** develop and implement a data retention policy and associated process for Business Customer Data, including submitted applications.

Business Customer Profile Data and Platform Usage Data

MBIE must ensure that it does not retain Business Customer Profile Data and Platform Usage Data for longer than it has a lawful purpose to use it. For Business Customer Profile Data, MBIE should set a retention period associated with the activity on that account. For example, this data could be deleted (and therefore accounts closed) after a period of 5 years of no activity. MBIE can retain Platform Usage Data indefinitely if it de-identifies the information (for example by removing identifiers such as customer account numbers, names, or IP addresses). Any retention periods set will also need to align to the government's General Disposal Authorities and any specific MBIE data retention and disposal policies.

Figure 9 – Sample data retention policy for Business Customer Profile Data and Platform Usage Data

Information	Minimum retention period	Maximum retention period	Disposal action
Business Customer Profile Data	For duration of business customer account	5 years after last action by customer	Contact business customer, then delete and close account
Platform Usage Data	None	5 years after last action by business customer	De-identify

Rec-012: MBIE **must** develop and implement a data retention policy and associated process for Business Customer Profile Data and Platform Usage Data.

6.3.5 Data access, use and disclosure rules

MBIE must ensure that the Business Connect team has a clear understanding of the ways it may, or may not, access, use or disclose the personal information stored and processed in

Business Connect. The specific boundaries will depend on the type of data and MBIE's status in relation to that data.

- **Business Customer Data and Application and Case Data**
  As a processor, MBIE must ensure that it does not access, use, or disclose Business Customer Data or Application and Case Data for any purpose other than delivering the services to business customers and GSPs. If it does, it will become a controller in relation to that information, and subject to the full force of the Privacy Act.

- **Business Customer Profile Data and Platform Usage Data**
  As a controller, MBIE can set its own rules in relation to the use and disclosure of Business Customer Profile Data and Platform Usage Data. However, it must ensure that it has a lawful basis under IPP 10 and IPP 11 to use or disclose this information in a specific way. The best way to ensure that particular uses and disclosures are lawful is to notify them to business customers in the Business Connect Privacy Statement.

MBIE should document the rules in relation to data access, use and disclosure in a Business Connect Data Use and Protection Policy, which reflects the dual status of MBIE under the Privacy Act, as outlined above. To ensure that Business Connect staff (and Datacom staff who are in supporting roles for Business Connect) are aware of this policy, MBIE should also develop and roll out privacy training specific to the Business Connect context (noting that generic MBIE privacy training will not be sufficient in this case).

Rec-013: MBIE **should** develop a **Business Connect Data Protection and Use Policy** to set guardrails on access to, use of, and disclosure of data for the Business Connect team.

Rec-014: MBIE **could** consider developing a privacy training programme specific to Business Connect, to embed the Business Connect Data Protection and Use Policy.

See Rec-009, which relates to updating the Business Connect Privacy Statement.

6.4 Opportunities for Business Connect to enable GSP privacy practice

As noted throughout this PIA, GSPs are responsible under the Privacy Act for ensuring that their services comply with the IPPs. This is also reflected in the contractual documents - clause 3(f) of the Host Agency – Client Agency MoU states that the GSP is responsible for ensuring the privacy and security of a service, and clause 9 of the Client Agency End User Terms states that the GSP must comply with the privacy responsibilities outlined in the Product Overview.

However, MBIE has an opportunity to use Business Connect to assist GSPs to better comply with privacy requirements, through processes, tools and functionality. In doing so, MBIE does not assume any liability under the Privacy Act for the service or the GSP's general compliance,

but it will be able to leverage privacy compliance as an additional benefit of using the platform for service development and delivery.

GSP considerations in relation to compliance with the IPPs are summarised at section 5. Some IPPs are more relevant than others, or more amenable to being enabled by Business Connect tools and functionality. These are outlined in more detail below.

Because MBIE will continue to have a role in assisting GSPs to develop their services, providing a support and guidance role and building forms and other components on the GSPs' behalf, there is an opportunity for MBIE to insert privacy criteria into the service development process. This could be achieved by developing a Business Connect Client Agency Privacy Checklist. A draft checklist is provided at Appendix 2, and the key risks it should address are outlined below.

Rec-015: MBIE **could** develop and implement a **Business Connect Client Agency Privacy Checklist** to promote privacy compliance by GSPs.

6.4.1 Enabling better data minimisation practices (IPP 1)

The GSP must ensure that it collects only the personal information it needs to manage a specific service via Business Connect. This includes minimising the required fields to be completed within an application form and minimising the scope of documents a business customer is required to submit in support of an application.

See Rec-015 - The **Business Connect Client Agency Privacy Checklist** could include guidance on data minimisation.

6.4.2 Enabling clear privacy transparency (IPP 3)

The GSP must ensure that it is transparent with business customers about the personal information it collects for the purpose of a service. This includes ensuring that the business customer is aware which agency is collecting the information. At present, specific services within Business Connect are clearly branded according to the relevant GSP. This means it is clear to the business customer which agency is collecting their information. However, the services reviewed for this PIA included no specific privacy notices for the services, and/or links to the GSP's general privacy statements.

See Rec-015 - The **Business Connect Client Agency Privacy Checklist** could include guidance on privacy transparency, and a requirement to ensure that a service-specific privacy statement is included in the online application form.

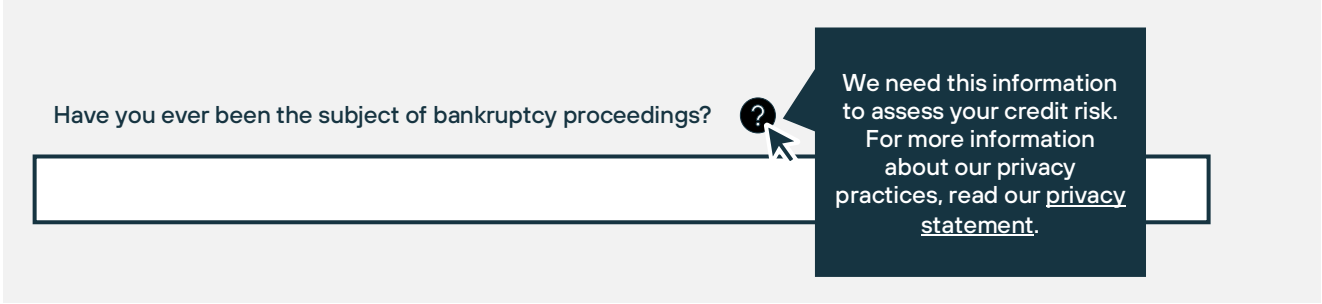
MBIE could provide GSPs with a simple privacy statement generator as part of the form components, which could assist GSPs to develop service-specific privacy statements, asking them questions to complete for the service. An example of a privacy statement generator can be found on the Privacy Commissioner's website - https://privacy.org.nz/tools/privacy-

statement-generator/. It is suggested that a tool such as this would be welcomed by GSPs, and particularly by smaller GSPs with less privacy resource available.

Rec-016: MBIE **could** consider developing a **Business Connect Privacy Statement Generator**, as part of the components offered to GSPs via Business Connect.

It may also be possible for Business Connect to enable GSPs to add a "tip" to certain questions in service forms, such as where a service is asking a business customer to provide sensitive information, or information they might not expect to be asked for. The tooltip could be used to quickly explain what the information is required for, and link business customers to a full privacy statement. For example:

Figure 10 – Sample privacy tip



Rec-017: MBIE **could** enable GSPs to add "tips" to forms to provide business customers with clarity about the collection of sensitive or unexpected personal information.

6.4.3 Enabling business customer privacy rights (IPPs 6 & 7)

The GSP must ensure that business customers can access and correct their information. Before an application has been submitted, business customers will be able to access and correct their information directly via the user portal. However, once an application has been submitted, it will not be possible for a business customer to correct it via the portal. Therefore, GSPs will need to ensure that they have internal processes in place to enable the correction of applications once submitted, and that these are clear to business customers.

See Rec-015 - The **Business Connect Client Agency Privacy Checklist** could include guidance on ensuring business customer privacy rights are enabled and respected, including by ensuring there is a prominent GSP contact link in service forms.

6.4.4 Promoting compliant data retention practices (IPP 9)

The GSP must ensure that it does not retain Application and Case Data in its backend systems for longer than it has a lawful purpose to use it. For GSPs, this will involve a consideration of any minimum data retention requirements set by relevant laws or regulations (including the Public Records Act or relevant General Disposal Authorities), and maximum data retention requirements set by its legitimate use of the information for the purposes of the service.

See Rec-015 - The **Business Connect Client Agency Privacy Checklist** could remind GSPs that they should set data retention policies for Application and Case Data, and that Business Connect is not a replacement for their own backend systems.

6.4.5 Promoting compliant data use and disclosure (IPPs 10 & 11)

The GSP must ensure that it uses Application and Case Data only for the purpose of deciding on a service application, or in other ways as notified to business customers in its privacy statement. The GSP must also ensure that it does not disclose Application and Case Data, unless that disclosure is directly related to the processing of that application, and has been notified to business customers in its privacy statement.

See Rec-015 - The **Business Connect Client Agency Privacy Checklist** could remind GSPs to ensure that they use and disclose Application and Case Data only in the ways they have notified to business customers in their privacy statement.

6.4.6 Providing threshold guidance for privacy risk assessments

As noted above, the Business Connect contractual documents require GSPs to consider completing a PIA on a service where necessary. However, the requirement for a PIA should be risk-based. For example, if a GSP is simply transferring an existing service to Business Connect, and not changing that service (or the ways personal information will be used) in any way, a full PIA may not be required. By contrast, if a GSP is developing an entirely new service for use in Business Connect, that includes the collection of sensitive personal information or may capture information about consumers, then a full PIA may be warranted.

As part of its Business Connect service, MBIE could assist the GSP to decide whether a full PIA might be necessary. This could be achieved by providing GSP's with threshold guidance on when a PIA might be warranted. MBIE will need to be absolutely clear that such guidance is not legal advice, and that the GSP will need to consult with its own Privacy Officer before deciding whether a PIA is required.

See Rec-015 - The **Business Connect Client Agency Privacy Checklist** could remind GSPs to consider whether a full PIA is required on a service, and provide threshold examples to assist them to take a risk-based approach.

Appendix 1: Information gathering

Stakeholders interviewed

- Daryl Pettitt – Director, Business Connect
- Mark Davis – Product Delivery Lead, Business Connect
- Will Chaney – Commercial Consultant
- Jacob Hutchinson – Datacom Business Manager
- Shelley Campbell – Product Owner, Business Connect
- Aaron Yee – Business Connect Technical Lead
- David Birdsall-Smith – Senior Solicitor, MBIE
- Nicole Rushton – Senior Solicitor, MBIE
- Dan Ormond – Latitude Strategy & Communication
- Bryre Patchell – Group Manager, Business Improvement and Innovation, NZ Customs Service
- Daine Bigham – Security Consultant, Helix Security Services
- Sonya van Eekelen – Director, Total Height Safety (business user representative)

Documents reviewed

- Business Connect Business Case for Phase 2
- Excerpts from Business Connect Vision PowerPoint presentation
- Business Connect Privacy Impact Assessment (PIA) September 2019
- Business Connect Technical Overview
- Business Connect Certification and Accreditation Summary November 2022
- Business Connect Product Overview December 2022
- Statement of Work 23 – Services SoW for Service Management – Business Connect Platform
- MBIE – Business Connect – MoU for the development of New Service(s) Final Template
- MBIE – Business Connect – End User Agreement – Final Template
- MBIE – Business Connect – Variation and renewal of Agreement FINAL (Datacom Agreement)
- Pega Cloud Risk Assessment
- Business Connect Team Organisational Chart
- 2022 Business Connect Advisory Board Terms of Reference
- Business Connect – Roles and Responsibilities under MOU May 2022
- Business Connect Programme – RACSI v2.5 (FINAL) Nov 21
- Business Connect Terms of Use – from https://www.businessconnect.govt.nz/terms-of-use, as at 15 February 2023
- Business Connect Privacy Statement – from https://www.businessconnect.govt.nz/privacy, as at 15 February 2023
- Various webpages of businessconnect.govt.nz, to understand structure and navigation of Business Connect portal

Appendix 2: Business Connect Client Agency Privacy Checklist

Client Agency Privacy Checklist

This checklist has been developed by Business Connect to assist Client Agencies to meet their obligations under the Privacy Act and Information Privacy Principles when developing services for use on the Business Connect platform.

This is not legal advice, and should not be relied upon solely to meet your Privacy Act obligations. Always talk to your Privacy Officer before finalising your service requirements and launching your service on Business Connect.

Business Connect is about businesses, so why do we need to care about privacy?

Because Client Agencies use Business Connect to deliver services to businesses, not consumers, a lot of the information collected through the platform will not be personal information. However, there are several circumstances in which Client Agencies will be collecting personal information about individuals, including:

- If a business customer is a sole trader, in which case information about their business is also personal information about them.
- If a business customer is required to provide their own personal information as part of the process, such as their name, contact details, or information about their directorships.
- If a service is targeted at consumers, or could also be used by consumers.

For these reasons, it is important to consider privacy every time when developing a service for use on Business Connect.

Privacy Checklist for your service

Have you considered what personal information you really need to deliver your service, and ensured that the forms you are developing request only that information? ☐

A Client Agency must ensure that it collects only the personal information it needs to manage a specific service via Business Connect. This includes minimising the required fields to be completed within an application form and minimising the scope of documents a business customer is required to submit in support of an application.

Have you ensured that you are providing adequate privacy transparency to business customers in relation to your service? ☐

A Client Agency must provide a clear privacy statement to a business customer about the personal information it is collecting, how it will be used or shared, and how a business customer can access or correct it. This privacy statement should be included as a link in the service form(s). Client Agencies can use the Business Connect Privacy Statement Generator to create a service-specific privacy statement, or provide a link to their general privacy statements (as long as they cover the specific service). Client Agencies can also add 'tips' to questions in their service forms to help business customers understand why certain data elements are required (such as sensitive information)

Have you ensured that business customers will be able to access and correct the Business Connect data you hold about them in your backend systems? ☐

A Client Agency must ensure that business customers can access and correct their information. Before an application has been submitted, business customers will be able to access and correct their information directly via Business Connect. However, once an application has been submitted, it will not be possible for a business customer to correct it this way. Client Agencies need to ensure that they have internal processes in place to enable the correction of applications once submitted, and make these clear to business customers via Business Connect.

Have you developed a data retention policy for the Business Connect data you hold in your backend systems? ☐

Remember, the Business Connect platform is a transactional system only. It is not intended to be the system-of-record for a Client Agency's service data. This means a Client Agency must ensure that it retains a copy of Business Connect data within its own backend system-of-record. The Client Agency is responsible for ensuring that this data is retained only for as long as it is needed for a lawful purpose. this will involve a consideration of any minimum data retention requirements set by relevant laws or regulations (including the Public Records Act or relevant General Disposal Authorities), and maximum data retention requirements set by its legitimate use of the information for the purposes of the service.

Have you considered how you will use or share Business Connect data for the purposes of your service, and ensured that business customers have been informed about this in your privacy statement? ☐

A Client Agency must ensure that it uses Business Connect data only for the purpose of deciding on a service application, or in other ways as notified to business customers in its privacy statement. A Client Agency must also ensure that it does not disclose Business Connect data, unless that disclosure is directly related to the processing of that application or has otherwise been notified to business customers in its privacy statement.

Have you considered whether a full Privacy Impact Assessment (PIA) might be warranted for your service? ☐

Where a Client Agency is transferring an existing service to Business Connect, it may not need to complete a full PIA. However, a full PIA might be warranted if the Client Agency is (for example):

- developing an entirely new service;
- significantly changing an existing service;
- considering collecting sensitive personal information (such as financial information or health information) as part of the service; or
- intending to make a service available to consumers.