Independent PIA of Business Connect

The Ministry of Business, Innovation and Employment (**MBIE**) asked Simply Privacy to conduct an independent Privacy Impact Assessment (**PIA**) of the Business Connect platform. The PIA was intended enable the growth and evolution of Business Connect in a way that will meet the needs of Government Service Providers (**GSPs**) and the business community, while protecting and respecting the personal information processed through it.

This is a summary of our PIA and MBIE's responses to it, which was completed on 6 August 2024. A glossary of the terms used in this summary is included at Appendix 1.

Business Connect

MBIE developed Business Connect in 2019 following research which showed that businesses had a generally poor experience of dealing with government application processes. The purpose of Business Connect is to provide business and government with a common platform to enable GSPs to digitise and streamline business services and interactions across central and local government. To achieve this, Business Connect provides GSPs with the form building (using either "Platform Forms" or "Forms as a Link") and case management tools required to deliver end-to-end services.

Business Connect is delivered via a "shared services" approach to procuring, hosting and maintaining the platform. The approach enables a one-to-one contractual relationship between a Host Agency, MBIE, and the primary service provider, Datacom, and the delivery of platform-related services to each GSP via the Business Connect End User Terms. 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.

The shared services approach used for, and high-level data flows enabled by, Business Connect are set out in Appendix 2.

Scope of the PIA

The PIA process involved reviewing the Business Connect platform, the personal information affected, and how that information was to be collected, used, stored and shared. We completed the PIA by reference to the Privacy Act's information privacy principles (**IPPs**) the principles contained in the government's Data Protection and Use Policy (**DPUP**), and relevant regulatory developments (including in relation to the use of biometrics and artificial intelligence).

We considered:

- The privacy implications for MBIE as Host Agency in relation to delivering the Business Connect platform for GSPs.

- The privacy implications of using service providers to deliver the Business Connect platform.
- Potential opportunities the Business Connect platform offered for enabling privacy best practice by GSPs, as part of the overall service offering.

We did not consider:

- The technical security risks created by Business Connect. While security is an important element of the privacy framework, and the PIA considered high-level security risks, this was not a security assessment.
- Privacy compliance by individual GSPs in relation to the services they deliver via Business Connect, other than where this was directly relevant to the Business Connect platform.

Privacy Act status of each Business Connect Stakeholder

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.[1] This distinction helps us to understand how privacy rights, responsibilities and liabilities attach to various agencies involved in a process.

The status of Business Connect Stakeholders is somewhat complex, and will depend on the nature of the services being delivered by each, the type of personal information being processed, and the purposes of this processing. We found 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.
- **Customers** are 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.

[1] See section 11 of the Privacy Act. 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.

Overall privacy risk profile for Business Connect

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. However, there are 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 slightly elevates the overall privacy risk profile for Business Connect, and the findings and recommendations made in the PIA reflected this.

	Where a 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.
	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	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 customer. For example, if the 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.
	Some services, such as the registration of trademarks with IPONZ or applications for alcohol licenses, 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.

Business Connect impact GSP compliance with the IPPs

IPP	Impact
1. Collect only personal information that is necessary for a lawful purpose	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 customer is required to submit in support of an application.

IPP	Impact
2. Collect personal information directly from the person concerned	The GSP must ensure that it collects personal information directly from the 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 customer via the application process. This complies with IPP 2.
3. Tell people why personal information is required, how it will be used, and who it may be shared with	The GSP must ensure that it is transparent with customers about the personal information it collects for the purpose of a service. This includes ensuring that the 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 customer which agency is collecting their information. The services reviewed for the PIA included no specific privacy notices for the services, or links to the GSP's general privacy statements. GSPs will need to ensure that this is done.
4. Collect personal information in ways that are lawful, fair, and not unreasonably intrusive	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.
5. Take reasonable steps to keep personal information safe and secure	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. **See below for more information on security and service provider risk.**
6. Let people access their information	The GSP must ensure that customers can access their information when they request it. This will generally be enabled by the Business Connect platform itself, which allows 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.
7. Let people correct their information	The GSP must ensure that customers can request to correct their information. Customers will be able to access and correct their profiles and draft applications directly via the user portal. However, once an application has been submitted, it will not be possible for a 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.

IPP	Impact
8. Take reasonable steps to check personal information is accurate before using it	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 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 customer to the correct business, via RealMe and NZBN.
9. Don't retain personal information for longer that it's needed for a lawful purpose	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. Each GSP will also need to decide how long Application and Case Data should be retained on its behalf within Business Connect. This should reflect the data retention rules it develops for its backend systems but, noting that Business Connect is not intended to be the GSP's system of record, could be shorter. MBIE will facilitate these retention periods on behalf of the GSPs.
10. Use personal information only for the purposes it was collected	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 customers in its privacy statement. **See below for more information on data use by MBIE, as Host Agency.**
11. Don't disclose personal information, unless an exception applies	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 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). **See below for more information on data disclosure by MBIE, as Host Agency.**
12. Only disclose personal information to overseas third parties if	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

IPP	Impact
it is subject to comparable privacy safeguards	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.
13. Only assign unique identifiers if you need to, and don't assign another agency's unique identifier	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 (though an application can proceed without one). 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.

Service provider risk

We reviewed all the relevant contractual agreements relating to Business Connect, including agreements between GSPs, MBIE, and the service providers, and universal Service Terms provided by AWS. In this review, we assessed how well each agreement reflected the status of the parties under the Privacy Act (as controller or processor), ensured that controllers retained control of the data, and addressed the privacy and security assurances that are now standard in these sorts of arrangements.

Overall, we found that the combination of contractual agreements, 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. We recommended to MBIE that some improvements could be made to some of the agreements to ensure that there was clarity in respect of important data rights and responsibilities. MBIE made the recommended changes where this was possible, and will continue working through the recommendations as the relevant agreements come up for review.

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. This 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.

Business Connect data will be stored at rest in **Australia**.[2] 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.

However, we recommended that Business Connect data should be moved to the NZ AWS region once this was available, as it would significantly reduce jurisdictional risk and address other concerns including in relation Māori data sovereignty. MBIE accepted this recommendation, and will implement it once this is possible.

Data security

Security is a critically important risk to manage in the context of a Platform-as-a-Service offering. 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;[3]
- Pega will (and is required by contract to) ensure technical security measures are in place and operational in respect of the Pega Platform;[4]
- 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 PIA was not a security assessment. However, as part of the overall PIA process, we reviewed the relevant security documentation and interviewed IT Security staff. On the basis of

[2] 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.
[3] More information about AWS' technical and other security measures can be found at https://aws.amazon.com/compliance/data-protection/.
[4] 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.

this information, we found that MBIE appeared to be taking reasonable steps to ensure that platform security risks were 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.

Data access and use by MBIE

We found that, given its mixed status in relation to Business Connect (as a processor and controller), MBIE would need to ensure that its staff had a clear understanding of the ways they 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.

We recommended that 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, we also recommended that MBIE should develop and roll out privacy training specific to the Business Connect context. MBIE accepted both of these recommendations, and is working to implement these.

Enabling GSP privacy compliance

GSPs are responsible under the Privacy Act for ensuring that their services comply with the IPPs. This is reflected in clause 9 of the Business Connect End User Terms, which states that the GSP must comply with the privacy responsibilities outlined in the Product Overview.

However, we found that MBIE had an opportunity to use Business Connect to assist GSPs to better comply with privacy requirements, through processes, tools and functionality. Because MBIE has 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, including in relation to:

- enabling better data minimisation practices;
- enabling clear privacy transparency, through both guidance and form functionality;
- enabling customer privacy rights, such as access and correction;
- promoting compliant data retention practices; and
- promoting compliant data use and disclosure.

We recommended that MBIE should develop a Business Connect Client Agency Privacy Checklist, and MBIE agreed to do so. The checklist is available on **businessconnect.govt.nz**.

Who is Simply Privacy?

Simply Privacy is one of NZ's leading privacy consultancies, providing privacy strategy, risk analysis, and consultancy services to public and private sector agencies in NZ and around the world. Simply Privacy's directors have previously held senior roles with the Office of the Privacy Commissioner, and senior privacy sector privacy roles. Simply Privacy has provided PIA and other assessment services to numerous companies and government agencies on varied projects and processes. For more information about Simply Privacy, go to **simplyprivacy.co.nz**.

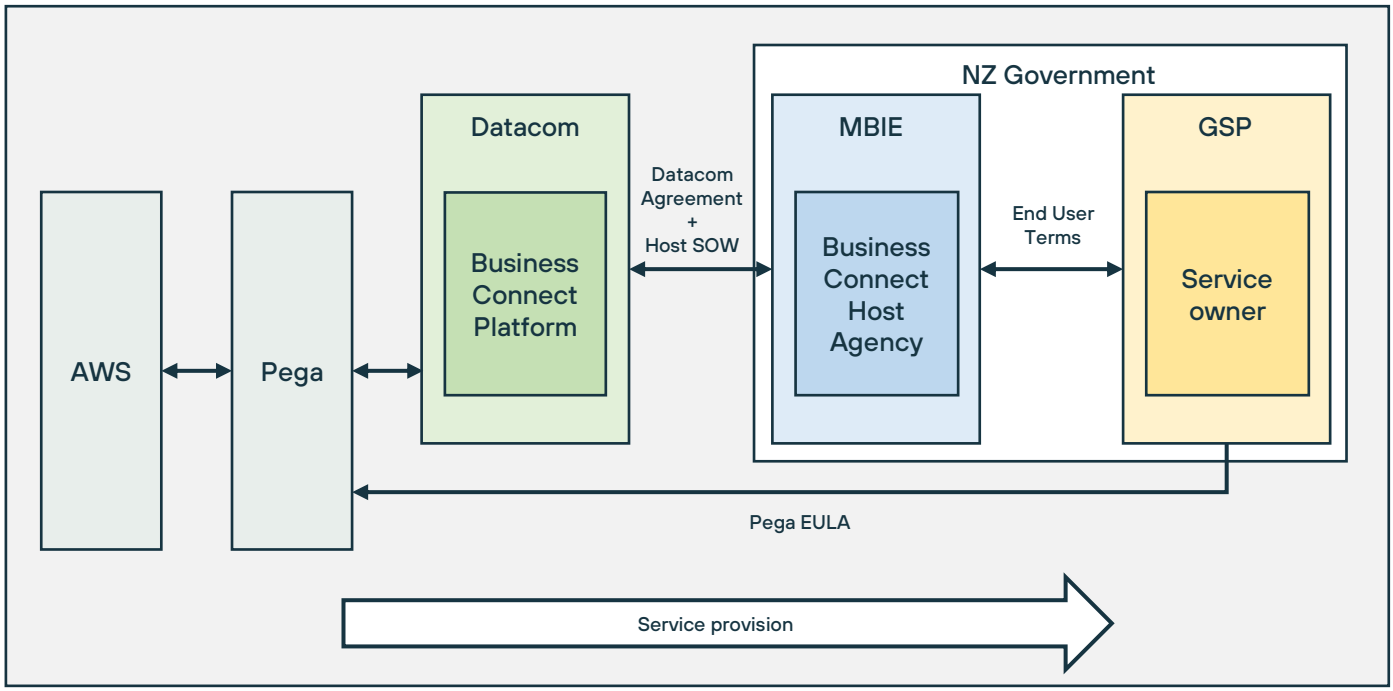
Simply Privacy

Appendix 1: 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 of the Business Connect PIA, including the Host Agency, GSPs, business customers, Datacom, Pega Systems, and AWS.
Customer	The 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 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 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 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 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.

Appendix 2: Shared services and high-level data flows

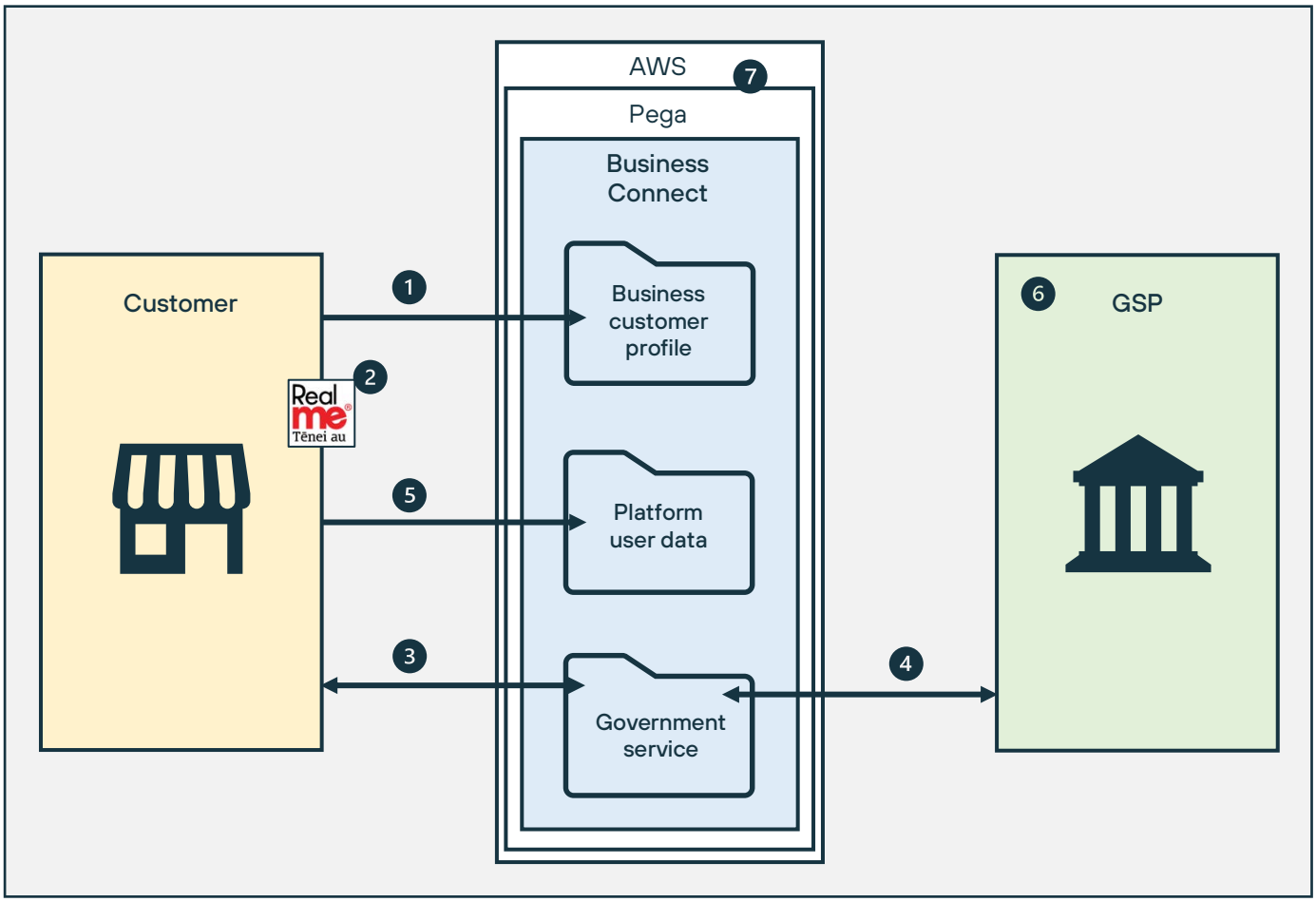
Shared services approach



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.
Customer	This is the person who uses the Business Connect platform to engage with GSP services. The customer could represent an incorporated business or a sole trader, or occasionally an individual consumer, and a customer might assign several staff to manage that business' Business Connect account. Current 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

Stakeholder	Role
	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.

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. 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 customer can then make service applications, using the forms required by the relevant GSP for that service. The customer can also upload documents in support of an application. Within the platform, the 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. An application submitted by a customer can be viewed by any other Business Connect user who has authority in relation to that customer's business.

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 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 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 customer.