DATA REPUBLIC

Australia-Singapore Digital Economy Agreement

Submission on Cross Border Data Exchange

Contents

Executive Summary 3

The Data Economy Opportunity 4

Key themes, challenges and areas for improvement: 5

1 Understanding types of data sharing 5

2 Personal Information v Aggregated, anonymised data 6

3 Smart technology and Smart regulation - harmonisation and interoperability 7

4 A balanced approach to Data Sovereignty 8

5 Responding to consumer consent expectations 10

Considerations for an Algorithm-to-Data based Data Free Trade Agreement 11

Exploring opportunities for Data Republic to facilitate cross-border data trade 13

How would the POC projects work? 15

Advisory support 15

Data Republic's engagement in Australia and Singapore: 16

Concluding Note 17

Executive Summary

Data Republic welcomes the opportunity to make a submission to the Department of Foreign Affairs and Trade (DFAT) on the Singapore-Australia Digital Economy Agreement. We recognise that this will be a new kind of Agreement for Australia and Singapore, setting benchmark rules to facilitate global digital trade.

At Data Republic, we firmly believe in the need for greater global data liquidity so that wiser decisions can be made and better outcomes delivered for individuals, businesses, and society – goals which require the development and adoption of trusted standards for cross-border data sharing.

Over the past four years, Data Republic has worked with industry and government across Australia and Singapore to both develop and implement best-practice technology standards for the secure governance, licensing orchestration and protection of privacy when sharing data between organisations. This has provided us with unique perspectives and value-add technology capabilities which can be readily applied to the DFAT Singapore-Australia Digital Economy Agreement policy development process.

The following paper explores Data Republic's recommendations in relation to a selection of topics that are included in the scope of negotiations with Singapore:

- cross-border data flows and location of computing facilities, including in the financial sector;
- artificial intelligence;
- data innovation, and
- protection of personal information, including across borders

Due to our experience in data exchange within Australia and Singapore, Data Republic is well positioned to assist DFAT from an advisory and technology perspective with this initiative. We stand fully aligned with DFAT's intention to create a repeatable model to accelerate Australia and Singapore's leadership in the global data economy.

Thank you for your consideration,

Danny Gilligan

Danny Gilligan,

CoFounder & CEO, Data Republic

The Data Economy Opportunity

Data Republic believes that data is the single biggest lever for micro-economic and social reform in the next two decades. Consequently, we see an opportunity for the emerging data economy to rapidly develop into the most material new sector of the economy across that period.

We define the data economy as the trade in data between organisations and/or governments, domestically or internationally, and the derivative data products (algorithms, insights, applications) that arise from that previously unavailable flow of data. The data economy is comprised of organisations and governments that are able to provide personalisation of services through data insights as well as develop data-driven solutions to old (and emerging) problems. It deals with productivity issues in the private sector (personalisation, risk, identity, supply chain efficiency, decisioning, development of artificial intelligence applications) and social reform issues across the public sector (policy reform, allocation of resources, programme efficiency).

We acknowledge that in this very new domain, there is a fundamentally differentiated global landscape; between those nations that produce high volumes of data records and those that process (or value-add) to datasets; those with strong privacy laws and those with none; those with open data strategies and those with closed ones; and between those nations that have developed sophisticated regulatory and industry development policies in response to this changing data world and those that are lagging behind.

The data economy represents a significant global economic, political and social opportunity, however the enabling regulatory environment plays a critical role in ensuring how well this opportunity is leveraged for national and cross-border economic growth.

Within the current global landscape of varied regulatory settings and “data production” vs. “processing” profiles, Data Republic considers Singapore and Australia as two of the most advanced data economies. Both are built on strong privacy foundations (Privacy Act 1988 and PDPC 2012), both have strong fintech and startup ecosystems, and both have progressive open data strategies (Consumer Data Right in Australia and Data Portability (in draft) in Singapore).

The core opportunities we see for Singapore and Australia in a Digital Free Trade Agreement are to:

- Harmonise critical privacy and regulatory issues with regard to data to enable a common/interoperable “leading light” approach that balances privacy and innovation.
- Develop common technical and policy approaches to facilitate functional cross-border data trade in a way that recognises and is compatible with emerging data sovereignty regulatory trends.
- Provide a highly functional model for other markets to adopt and thereby catalyse global trade in data. Lead by example.

Key themes, challenges and areas for improvement:

1 Understanding types of data sharing

Since launching in 2016, Data Republic's technology has been rapidly adopted by major banks, airlines, retailers, insurers and governments across Australia, Singapore and the United States to govern multi-party data collaboration and licensing. We currently work with organisations across the full spectrum of data sharing maturity.

For the purposes of this submission, there are three major kinds of data-sharing worth understanding and considering when designing cross-border data policy:

A) **Straight Algorithm to Data** – this is where an algorithm, data product, or AI/ML application from one market moves into another market. This can be achieved with minimal material changes to regulatory settings today, however increasing confidence will need to be given to data regulators that data is not being "off-shored" as a result of access given to that algorithm. Because this is the simplest, lowest risk approach, our view is that common infrastructure, taxonomies etc that form part of a data free-trade agreement can maximise the potential for safe data liquidity. In this instance, markets that develop data-driven applications can then sell those apps into other markets, while data remains where it is (ie sovereign) and the trade can occur at the application layer. This is the same model that has effectively worked in the consumer domain with apps on IOS or Android.

B) **Federated analytics** – this is where an algorithm, data product, or AI/ML application needs to run on multiple data sets that are usually the same kind of data. An example here could be an anomaly algorithm that runs on airline engine IOT data, where a global component supplier may want to run across multiple airline data sets across several markets. Again, this can be achieved in a similar manner to the construct above, as long as common infrastructure, taxonomies etc exist per industry vertical, use case type etc.

C) **Joined data sets** – this is where two or more different data sets need to be brought together to enable a new insight to be discovered from the combined data. This represents a complex problem for cross-border data sharing as at least one of the data sets needs to move from one jurisdiction to another (as is the case for companies today). It is not possible to solve for this whilst strictly honouring data sovereignty. However, we believe it is possible to create approved, regulated processes and channels which solve as much as is possible. This would include consideration of a temporal landing zone for a joined data set, where data is moved from one jurisdiction to another, via an approved channel, held temporarily for processing with another domestic data set and then having the output (derivative data product) leave and the inbound data set deleted. This would be the equivalent of an international airport where inbound visitors are not considered to have entered the country until they have passed customs but can be landed in a country. In the case of data, the inbound data set can arrive in a shared workspace on an approved basis (logged and approved trade), the data join processed, the output cleared to enter the jurisdiction and then the raw inbound data set deleted (or effectively refused entry).

2 Personal Information v Aggregated, anonymised data

There is a material difference between data-sharing that consists of aggregated, anonymised or pseudonymised data and that which requires matching of Personal Information (PI) to join a data record at an individual level.

Recently, the EU updated data policy to explicitly differentiate between the handling of PII and non-PII. New regulations, outlining mechanisms for the free flow of non-PII, allow EU members to store non-PII in any EU member state, and provide public authorities with guaranteed access to that data no matter where it is stored. According to the EU, the combination of the GDPR and the new regulations will "ensure a comprehensive and coherent approach to the free movement of all data in the EU."[1]Similar to the EU, we recommend that Australian data trade policy should clearly state the difference between PI and other data.

From our perspective, an ideal cross-border policy framework would liberalise the EU definition of PI to allow for both sovereign protection of individual personal information and the necessary flow of raw de-identified data (that does not include PI) for cross-border insight generation and matching.

PI sovereignty should be protected as an absolute. As it is highly likely that raw data, that does not specifically contain PI, could also be considered sovereign, we propose that the Australian definition of PI needs to be made more sophisticated and with greater nuance applied to the context of data. Currently PI is defined with reference to dated domestic privacy policies that do not adequately account for what has been made possible with technology over the past decade.

For instance, Data Republic has developed privacy-preserving matching technology that utilises a decentralised network of nodes and cryptographic techniques to allow PI to be matched between two organisations without said original PI ever leaving either company's firewall. By hosting a "Contributor node" of the network within a company firewall, a company can tokenise, hash, salt and shard the result into small fragments which are then pushed out of the firewall into a network of "Matcher Nodes". These fragments are distributed in a way to ensure that every node on the network only contains a small portion of the overall result, and the heterogenous nature of that matcher network means if any node is compromised, there is nothing that can be considered PI to obtain.

This private-by-design architecture which allows two companies to match individuals across datasets without PI ever leaving their individually secured environments (firewall) could equally be used for PI matching between two countries, so that the PI never leaves the sovereign control of either nation.

What is required is a recognition that such a process and the resulting mirrored PI fragments that exist in a matcher network shared between two markets do not constitute PI for the purposes of domestic Privacy Laws. The matching process could be considered the data equivalent of "international waters".

[1] "Free flow of non-personal data" policy, European Commission, updated June 2019, https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data

3 Smart technology and Smart regulation - harmonisation and interoperability

We have observed in the emerging domain of data, and in particular the regulation of data, a significant first-mover advantage for nations when it comes to data policy development and implementation. The EU implementation of GDPR is often talked about as the global standard for data protection and is the inspiration for the CCPA in California. In addition, the UK Open Banking Model has been well marketed as the standard for Open Banking globally.

In our view, neither the UK Open Banking regime or GDPR are (or more to the point, should be) the global standards for Open Banking or data protection. In each case, there are significant technical and systemic issues which undermine their purpose. In the case of UK Open Banking, the system is designed for the free-flow of raw banking and transaction data from one entity to another. Fintechs are eager to see drastic change so they can have access to a wide range of account data – everything from superannuation, credit cards, and rewards systems to mortgages, lines of credit, and insurance data. But it's important to consider the ramifications of allowing fintechs of all shapes and sizes unfettered access to high volumes of raw banking data. There are serious data security, privacy, and compliance implications for fintechs in most countries, and they will need to match the sophisticated data security systems and protocols that took banks years to define and implement.

It is not hard to imagine the oncoming challenge to regulators and banks when a fintech suffers a breach, releasing terabytes of data relating to thousands of individuals obtained from banks through the auspices of Open Banking. Many individual actions can produce large amounts of data, now no longer safe behind bank grade security. This creates systemic risk by unnecessarily increasing the amount of raw data in the ecosystem (replicating data and transferring data from high security banking domains to low security fintech startups).

As opposed to raw flows of data, an "algorithm-to-data" model, where approved algorithms are able to query the original dataset and return only approved outputs, would solve this issue effectively, allowing the same outcomes for consumers while providing both a greater level of consumer protection and less liability for Open Banking industry participants.

GDPR also has its issues. There are six lawful bases for processing personal information under the GDPR. In addition to processing with consent or for a contractual purpose, one of the lawful bases is where the processor has a "legitimate interest" in carrying out such processing activities. The term "legitimate interest" is left open to very broad interpretation by the processor themselves. Certain global social media giants have indicated in public statements that rather than consent, "legitimate interests" is their preferred basis for processing the personal information of users. In our view, this diminution of the importance of consent runs contrary to the expectations of consumers and is a potential flaw in GDPR (that is not to say that properly conceived, a "Legitimate Interests" or "Secondary Purpose", would not be desirable).
Another flaw in the GDPR approach is that it in some circumstances it is declarative of rights without establishing the technical framework for the realisation of those rights. Under GDPR, consumers have a right of portability. However, GDPR does not stipulate a practical standard for the operation of that right. This is in contrast with the Australian Consumer Data Right and the UK Open Banking regime which have both established standards bodies tasked with enabling the portability right in practice.

Notwithstanding the above outlined flaws, it is clear that GDPR and UK Open Banking have both been hugely successful national branding exercises in data policy. They have demonstrated the importance of moving quickly in response to shifting global sentiment and technology innovation. Fortunately, Australia and Singapore are well progressed in this space.

However, in our view there is more to be done and it is critical that Australia and Singapore work together to future-proof their respective policy foundations ahead of emerging data economy maturity shifts from intra-national data exchange and sharing to inter-national exchange and sharing. In order to achieve this, in our view the first steps are to ensure that the regulatory settings in Australia and Singapore are sufficiently flexible to be interoperable and enable controlled exchange of data.

The increasing in-bound interest that Data Republic has received from markets and governments other than Australia and Singapore (UK, Thailand, Indonesia, Malaysia, US, Canada, United Arab Emirates) demonstrates that there is a high potential for both regulatory harmonisation and interoperability, and commercial exchange. Specifically, we think there is enormous value in the recognition of the interplay between technology (what is possible) and policy (what is permissible) and that developing national data policy without this recognition is likely to position regional data economies to under deliver relative to their potential.

Specifically, we recommend a "policy proto-typing" approach be taken to developing the data-sharing component of a digital Free Trade Agreement. That is, outline a policy framework that can be tested in parallel with a practical Proof of Concept. The outcomes from this technology enabled approach can help inform a final policy position which gives greatest effect to the potential for a commercially implementable outcome.

4 A balanced approach to Data Sovereignty

Technological progress has facilitated the free flow of data around the globe, fuelling consumers' and businesses' insatiable appetite for digital services. However, it has also fuelled a fundamental economic imbalance between these all-powerful 'data processors' and 'data producers'—the countries, organizations and individuals from which the data or information is sourced.

If data is the new oil of the global digital economy, the growing movement towards data sovereignty represents an effort by its producers to rein in the massive imbalance in the consumption of their data. Long unregulated, the movement of data has become a key negotiating point in global trade agreements that are also being shaped by the dictates of ever stricter privacy laws. The result is new regimes of "data sovereignty" laws that treat data as a national asset—and recognise the risks of allowing it to be exploited by foreign interests that give little consideration for its provision.

Countries with Data Sovereignty laws generally justify such positions on the basis of privacy protection, national security and preserving the integrity of core systems by requiring them to be operated on-shore (i.e. no offshore cloud processing).

Countries can be separated into two categories with respect to data:

- Data Producers: typically are countries, with large populations, consumers of tech rather than producers, that generate vast amounts of data, do not have a sophisticated data processing industry (i.e. data science, AL/ML). Examples:
  - India
  - Indonesia
  - Vietnam
  - Brazil
  - Pakistan
- Data Processors: countries with thriving technology industries (or companies) that utilise data for value-added outputs relative to their own data producing population.
  - USA
  - China

- Singapore
- Sweden

Some Data Producer countries are also Data Processors (e.g. China, USA), however this is generally the exception to the rule.

The highest economic value in data is generated/exploited when large volumes of data are processed by Data Processors. Data Producers, on the other hand, generally realise very little economic gain from the production of data alone. The inverted input-to-value relationship between Data Producers and Data Processors incentivises Data Processors to obtain ever increasing amounts of data from Data Producers. Conversely, Data Producers are incentivised to limit flows of data to Data Processors in favour of becoming a Data Processor themselves.

In a real sense, Data Producers are just waking up to understand how fundamentally important data is as an asset and a resource—and that it should be thought of in the same way that countries think about any other natural resource.

Given the importance of data exchange to existing and emerging world economies, resolving the inconsistencies between various jurisdictions' data regulations will be a key feature of future trade negotiations. It is also likely to form an increasingly well-delineated part of national economic identities that are being reshaped by countries' participation in emerging data-driven economies.

If the 19th century was the age of industrialization and the 20th century the age of commercialization, the 21st century is shaping up as the age of data-driven expansion. Data sovereignty regulations will shape that expansion as competing national economic strategies set boundaries for the handling of this incredibly valuable and virtually unlimited resource.

While we recognise that while some countries are not in favour of data sovereignty as a policy response, it is the view of Data Republic that this is highly likely to be an inevitable global phenomenon (led by India, Indonesia etc.). Therefore, we strongly recommend that any policy frameworks that are developed need to be functional in a data sovereignty honouring world.

Australia and Singapore have the opportunity to combine Smart Technology and Smart Regulations to (A) meet the objectives of Data Sovereignty, while (B) enabling the export of data processing capabilities and data driven insights. The objective should be to develop the most 'free' trade in data possible in a data sovereignty honouring way. This will maximise the likelihood of regulatory mirroring of this construct in markets where sovereignty is key.

A. Red Herring Policy Example: Data Free Flow with Trust (DFFT)

One prominent approach to Data Free Trade is the concept known as Data Free Flow with Trust (DFFT). This approach underpins the "Osaka Track" launched by President Abe of Japan.

DFFT proposes free-flow of data between countries that have signed up to a shared framework of data and privacy protection principles in their regulatory framework (the trust element).

The DFFT approach has been rejected by key Data Producing nations including India, Indonesia and Egypt. The primary concern appears to be that DFFT disproportionately favours Data Processing nations over Data Producing nations as the value in the data flows out of the Data Producing nations and into the Data Processing nations.

The primary issue with DFFT is that when raw data flows out of a Data Producer to a Data Processor, the Data Processor has captured all of the value in the data and is able to

repeatedly exploit the data for that value without any requirement to transfer value back to the Data Producer (at least after the initial transfer of data to the Data Processor).

EXAMPLE: Data Producer might purchase a data set from a Data Processor for $100. The Data Producer now has that data set and can create data products from that data set and on-sell those data products to its customers for $100 per data product. If the Data Processor sells the data products 100 times, they have made $10,000 for an initial investment of $100.

B. **Opportunity: An alternative - Data Free Trade moves to outputs while honouring sovereignty**

An approach focused on outputs is built on reversing the current data flows from Data-to-Algorithm (move raw data to processor capability) to Algorithm-to-Data (move the data processing capability to the raw data). This approach would enable Data Producing nations to deal with Data Processing nations on a more even playing field and thereby encouraging greater freedom of trade around data.

The basic principles of the Algorithm-to-Data approach are:

- Raw data is not transferred, or is only transferred temporally to a secure space (from which it cannot be extracted in its raw form) and held temporarily until processing is complete then deleted.
- Value is created out of data by applying algorithms to the data to generate an output.
- The output may be extracted and transferred freely.
- The custodian of the raw data set retains control over the raw data set and is able to realise repeat value from the raw data set without having to transfer control of the raw data set to the Data Processor.

It's helpful to consider an analogy to airports and customs here where "diplomatic zones" for data could be created to enable raw data from one jurisdiction to be temporally landed to enable a joined data product to be created and "moved through customs" (governed flow into recipient data economy) while the raw data was "deported" (deleted).

5 Responding to consumer consent expectations

In the wake of high profile data breaches, leaks and media scandals, consumer data literacy has increased dramatically over the past three years. There has been significant push-back against corporations perceived misuse of personal data and consumers are now rightly demanding greater control and greater privacy protections with respect to the collection and use of their data.

At the same time, in an increasingly digital world individuals are also consuming more data-driven services and have higher expectations of personalised interactions with those services. This conflict (i.e. demanding more privacy while also demanding a company knows you better) presents a unique challenge for regulators.

At Data Republic, we do not think that privacy and data utility need be diametrically opposed. That's why we have developed technology which enables safe data movements/access while increasing the privacy and security protections around raw consumer data.

Data Republic's Senate Platform enables organisations to govern data movements and licensing from a private-by-design platform, transforming manual governance procedures and patched-together analytics solutions for multi-party data collaboration into simple, online workflows. Importantly, Data Republic's patent-pending privacy-preservation technology

enables organisations to match datasets across organisations (and borders) without exposing raw personal information. We are also in the process of developing an end-to-end consent management platform to enable consumer definition and dynamic control of consent as it relates to specific data movements between organisations.

Used in conjunction, Data Republic's technology suite will enable enterprise customers to integrate consumer consent frameworks into the orchestration and governance of organisational data sharing. Ensuring that the consent of customers is verified and applied to each B2B data collaboration.

Data Republic recommends that Australia's cross-border data policy and Singapore-Australia Digital Economy Agreement similarly considers how consent will need to be applied and managed across jurisdictions and specific data sharing use cases.

Considerations for an Algorithm-to-Data based Data Free Trade Agreement

Synthesising the above industry findings and recommendations, Data Republic proposes the following recommendations for consideration in the Australia-Singapore Digital Economy Agreement.

(1) Common foundational definitions for data-sharing

a. There is a need to harmonise on certain critical definitions and ideally taxonomies and to create space for those concepts with regard to the relevant domestic laws.
b. For instance, a recognition under a data Free Trade Agreement that PI which has undergone a technically rigorous process of tokenisation and sharding is not PI for the purposes of the Australian Privacy Act and Singapore Personal Data Protection Act and does not breach the concept of data sovereignty where it occurs through an approved channel would be critical to enabling cross-border data sharing.
c. Ideally, there would be space created to allow industry to harmonise on common taxonomies, permitted uses, simple consent definitions etc which would permit data products to move across borders with greater ease/less friction. This is not essential to the minimal functioning of a data Free Trade Agreement but would materially improve liquidity across markets over time. This could be completed on an Industry by Industry basis.
d. Further questions to be considered for cross-border harmonisation could include:
    - What constitutes raw data?
    - What constitutes personal data?
    - What constitutes a data product / value added data?
    - Categories of permitted uses for certain types of data?
    - Consumer consent taxonomies

(2) Approved trade channels and regulatory oversight

a. We envisage a process where cross-border trade in data is done through approved channels so that licensing of data and data products (insights, algorithms, applications) can be tracked, monitored and reported to create a transparent regulatory system.
b. These approved channels should be able to differentiate between raw data and a derivative data product/algorithm/application. We should encourage the flow of data products through approved trade channels while leaving PI and raw data in sovereign countries (to

the best extent possible). Alternatively, where raw data is permitted to flow, there is at least an auditable record of it.

c. Regulatory oversight of licenses – it should be possible to incorporate a regulatory body into a licensing process to provide pre-approval for a proposed cross-border data movement or transaction under consideration (i.e. DBS and WBC "agree" and both IMDA and ACCC "approve") or provide a reporting mechanism to log and surface all cross-border data shares if no pre-approval was needed.
d. These approved channels could enable concepts such as "international waters" for sharded PI matching and "diplomatic zones" for data temporally landed to enable a joined data product. Which could, in turn, be part of the regulatory tracking process above. It would even be possible to enable approved persistent Diplomatic Zones between countries so that permanent flow of de-identified data can occur (i.e. tracked, reported, approved, etc). A kind of "cooperative data warehouse/workspace".
e. These channels would also enable regulatory and taxation approaches to be streamlined to support the export of Data Product IP between countries (algorithm-to-data), for example; Analytical models, credit models, AI/ML applications, data applications.

(3) Recognition of different modes of data sharing

a. Recognition of the different modes and models of data-sharing would be needed to ensure regulation and policy reflected the different risks and issues associated with each kind of data sharing.

(4) Recognition of PI sovereignty

a. Our recommendation is that even if Singapore and Australia each have comfort with the idea of raw data flows between each nation, best attempts should be made to design a framework that honours emerging data sovereignty policy trends wherever possible.
b. This is likely to maximise the chance that anything developed under this digital Free Trade Agreement can be mirrored by other jurisdictions where data sovereignty is already a known or emerging issue.

(5) Collaboration on specific technology/policy interplays

a. New technological capabilities can be developed which will facilitate the potential for approved cross-border trade in data.
b. Data Republic is currently co-developing a Consent Management protocol for our enterprise clients in Australia and Singapore. Our objective in developing this across two markets in tandem is that we might create something that has appeal across all markets.
c. It is possible to then leverage that capability into a data Free Trade Agreement to facilitate a higher functioning version of cross-border data sharing.
d. Singapore and Australian governments could collaborate more formally on these kinds of opportunities with the current Consent Management protocol an immediate opportunity.

(6) Recognition and adoption of common infrastructure, technology principles

a. Similar to the Consent Management protocol above, technology infrastructure such as Data Republic's decentralised, privacy-preserving matching network could be recognised as approved common infrastructure under a data Free Trade Agreement.
b. Such an approach would allow for greater regulatory oversight as to data-sharing activity and trade occurring on that infrastructure as well as giving greater confidence to

enterprises and government organisations interested in conducting cross-border data sharing in the near term.

This would be the equivalent of the IMDA accreditation, by way of example.

- Agreed taxonomies of data types:
  - What constitutes raw data
  - What constitutes personal data
  - What constitutes a data product / value added data
  - Categories of permitted uses for certain types of data
- Agreed technology principles and policies:
  - Understanding that privacy-preserving / de-identified matching of data sets does not constitute disclosure of data (or PI) for the purposes of data sovereignty laws
  - Agreement on use of secure "Diplomatic Zones" for conduct of Algorithm-to-data processing activities

Exploring opportunities for Data Republic to facilitate cross-border data trade

As outlined above, Data Republic is supportive of a "policy proto-typing" approach being taken to development of the data-sharing component of a Singapore-Australia Digital Economy Agreement as this would enable policy frameworks to be tested in parallel with practical Proof of Concept projects. The outcomes of these cross-border POCs could then help inform a final policy position which supports the most commercially implementable outcome.

Data Republic is the platform of choice for governing inter-organisational data collaboration, already used by hundreds of organisations across Australia, Singapore and the United States to govern data sharing and collaborative analytics programs.

Data Republic can enable the first, regulated, industry led cross-border data sharing projects.

Participants in the proposed POC data sharing projects would utilise common infrastructure and technical approaches that already exist and are operating between both Singapore and Australia along with trial "DFAT approved channels" to give regulatory certainty to trial use cases. The following represents an initial straw man representation of some of the potential initial use cases that may be candidates for cross border data exchange.

Potential Use Case types:

A) Straight Algorithm to data
B) Federated analytics
C) Joined datasets

Category	Idea	Type
Corporate to Corporate	Commercial and residential property data to inform Singaporean investment into Australian development projects.	A

Corporate to Corporate	International sharing of credit score and fraud flags to improve expatriate process and reduce financial risk.	A
Corporate to Corporate	Trade finance data sharing to reduce debtor days in international financial transactions (cash flow improvements and lower trade risk).	A
Corporate to Corporate	Improving investment processes between countries, for example: ● International merger customer overlap assessment ● Additional data for cross border infrastructure investment ● Consulting opportunity gaps between countries	C
Corporate to Corporate	Predictive maintenance data sharing in relation to capital equipment in respective countries.	A
Corporate to Corporate	International conglomerate, with AU & SG customers, improve their ability to share customer data internally across borders.	C
Corporate to Corporate / Government	Materials and agricultural data sharing: ● Export tracking to establish provenance of goods and materials, including Trademark components ● Better understand buying preferences and patterns surrounding distribution of consumption and supply chain requirements	A/C
Government to Corporate	Tourism examples: ● Providing onward destination information to companies (e.g. Singapore Airlines) in order to segment customers and improve Australian Tourism marketing. Outcomes include: longer duration of stay, increased experiences during visit and broader end destination set. ● Share information to reduce country level travel insurance premiums	A/B
Government to Corporate	Tertiary education data exchange: ● Share information regarding shortages in the Singaporean tertiary education sector to improve Australian university performance in Singapore (James Cook University example) ● Certification of university courses and validation of education records to ensure background accuracy	A
Government to Government	Collectively improve Australian and Singaporean national health, including: ● Sharing information to restrict the spread of infectious disease ● Sharing vaccination information for expatriate transfers ● Testing health AI models and new research on either Austrailan or Singaporean national health datasets. ● Testing health treatments on larger sample sizes across combined population of AU/SG ● Price information sharing for medication and health supplies ● At risk population studies on a wider population and demographic (i.e. aging services, disability services)	A/B
Government to Government	Tax related items: ● Data sharing to check repatriated money at a citizen level	A / B

	• Corporate tax comparisons	
Government to Government	Climate data sharing, weather pattern and forecasting information with a short or long term impact on Australia and Singapore.	A / C
Government to Government	Policing data sharing • Criminal records monitoring • People trafficking information • Identity theft verification	A / C
Government to Government / Corporate	Personal data verification to expedite expatriate movement, including visa process and personal establishment (housing, travel insurance, health, banking, tax status and qualifications)	A / C

How would the POC projects work?

1. Data Republic would seek to enter into a Memorandum of Understanding (MOU) with both the Australian and Singaporean governments as an exploratory technology partner for the Singapore-Australia Digital Economy Agreement

2. Data Republic would seek POC programme funding from the Australian government to support:
    - An initial strategic advisory process; engaging parties from AU & SG governments, supporting the review and harmonisation of policies, confirming security protocols, developing collective initial use cases and benefits for Australian economy
    - Data Republic technology licensing and usage across selected POC projects
    - POC Programme Management between public and private participants in the Data Free Trade

3. Following acceptance of Data Republic's proposal on the above, our team would partner with the Australian government to rapidly prototype and execute approved POC use cases alongside public or private sector partners in Australia and Singapore.

Note: Private sector participants in Data Republic's existing governed data sharing ecosystems in Australia and Singapore can possibly be leveraged to accelerate outcomes for the POC programme.

Advisory support

Data Republic is also open to provide specific strategic advisory services, on a consulting basis, for:

- Best practices for public and private (government and corporate) cross border collaboration projects
- Research and taxonomy development for global data portability / interoperability standards
- Consent alignment - prototyping a cross-border common Open Source consent management protocols
- Objective setting to determine initial POC and ongoing use cases
- Knowledge transfer to enable public and private organisations to perform subsequent data exchange projects

Data Republic's engagement in Australia and Singapore:

- Data Republic is an early stage, home-grown Australian technology company with global ambitions. We have offices in Sydney, Singapore and Los Angeles, USA.

- Our leading technology enables organisations to govern data movements and licensing through a private-by-design platform, transforming manual governance procedures and patched-together analytics solutions into simple, online workflows. Importantly, Data Republic's patent-pending privacy-preservation technology enables organisations to match datasets across organisations (and borders) without exposing raw personal information.

- Data Republic focused on Singapore as its first key growth market outside of Australia because Singapore has clearly stated ambitions to lead the global data economy. Over the past 12 months, we have uncovered clear synergies in the way the Australian and Singaporean data economies operate. Not only with respect to the size and sophistication of the Singapore market, but also the shared legal and cultural prioritisation of functional, citizen-centric privacy policy.

- In our experience, Singapore has been a relatively easy market in which to become established, conduct operations, employ staff and deliver products and services. However, as with all things, there are many opportunities for improvement and our experiences to date have given us a unique insight on ways in which the Singapore and Australian trade relationship could be strengthened for both countries' benefit.

- Data Republic was founded in Australia in 2015 and raised Series A investment from tier one Australian corporates including Westpac Banking Corporation, National Australia Bank, QANTAS, with ANZ Bank also investing in a Series AA round.

- In December 2018, Data Republic completed a further capital raise (Series B) with follow-on investments from WBC and ANZ, as well as new investment from tier one Singapore corporates, Singtel and Singapore Airlines and Singapore based VC, Qualgro.

- The presence of these established Singaporean and Australian corporate giants on the capital table of a start-up like Data Republic is evidence of the shared challenges to which Data Republic is a solution. The governed, secure, auditable and privacy compliant exchange (or sharing) of data between organisations.

Concluding Note

Data Republic is open to continuing exploratory discussions on the above-outlined recommendations.

We thank the Department of Foreign Affairs and Trade (DFAT) for the opportunity to make a submission on the potentially ground-breaking Singapore-Australia Digital Economy Agreement.

Please direct any follow-up questions or queries to enquiries@datarepublic.com or visit www.datarepublic.com for further contact information.

Kind Regards,

Danny Gilligan,
CoFounder & CEO, Data Republic