



Australian Government Data Sharing & Release Legislation

Response to Issues Paper

SUMMARY

Equifax welcomes the opportunity to contribute to the development of the Australian Government's Data Sharing & Release Legislation. As a major partner with government on the effective use and release of public data, we bring deep experience and expertise on how to best use data to support the efficient delivery of government services.

We support the implementation of this new framework, including the purpose test and the *five-safes* framework. Key to making this data sharing and release framework work will be the role of the National Data Commissioner (NDC).

The NDC will set the tone for how key stakeholders interact in the system – and the guidance developed will have a direct impact on how the system functions between the public and private actors in the system.

EQUIFAX

At Equifax we power the world with knowledge. Equifax is a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to empower organisations and individuals around the world, by transforming knowledge into insights that help make more informed business and personal decisions.

Equifax empowers customers with information they can trust. We are Australia's oldest credit data and analytics provider, with over 50 years of local experience and 120 years of global expertise. Established as the Credit Reference Association of Australia in 1967, then as Veda and now Equifax, we have strong discipline in governance across the data lifecycle. We have a strong familiarity with the privacy regulatory framework, both the Australian Privacy Principles generally and also with specific pieces of regulation, such as the operation of Part IIIA of the Privacy Act 1988, or state tenancy register laws.

We live in a connected world; a world where decisions by both businesses and consumers rely on fast, accurate data. We know that more accurate data will lead to better business decisions. The Equifax consumer credit bureau is regulated by Part IIIA of the Privacy Act. We are the trusted custodians of 16.5 million Australian consumer credit reports, and operate a range of businesses that seamlessly facilitate productivity across the economy.

We also help consumers through a range of personal solutions that give consumers more control over their financial wellbeing.

We welcome the opportunity to contribute this submission to the Issues Paper consultation on the proposed Data Sharing and Release Legislation.

DATA SECURITY IS KEY

Globally, the Equifax network is reviewed on a continual basis by external security experts who conduct intrusion testing, vulnerability assessments, on-site inspections, and policy/incident management reviews.

To ensure data is secure, we use some of the best security techniques to protect it: encryption, tokenization, masking, encryption in motion, and encrypting at rest.

We also approach the systems and processes around data security as a key component of our security strategy. Only authorised employees are granted access to personal data. We train our employees who handle personal information to ensure it is handled appropriately. Our procedures ensure that personal data is only made available to employees where necessary. We audit and monitor our employees' access to, and handling of, personal information.

Access by our customers to personal information held by Equifax is available by subscription only and is tracked and recorded. Access is subject to contractual terms and conditions. Access to other personal information is subject to consumer consent, or is publicly available, or is subject to contractual terms and conditions. These include compliance with the *Privacy Act 1988* and other relevant legislation.

We are a member of the Australian Securities and Investments Commission (ASIC) Business Advisory Committee. We are currently the largest ASIC approved information broker, and we contributed financially and were a founder of the ASIC information broker service.

Equifax is an approved organisation with the Australian Financial Security Authority (AFSA) for access to the Personal Insolvency Reporting Service, and we are an approved AFSA B2G client, providing searches against the National Personal Insolvency Index. We are a member of the AFSA Personal Property Securities Register (PPSR) Stakeholder Forum and Operations Forum, and an approved AFSA B2G client providing searches and lodgments to the PPSR. We are one of the largest PPSR search providers.

Equifax is authorised by the Department of Home Affairs as a Gateway Service Provider to the department's Document Verification Service, and the Australian Criminal Intelligence Commission's National Police Checking Service.

We are also an organisation prescribed under the Electoral and Referendum Regulation 2016 to access the Commonwealth electoral roll, and an approved land titles information broker with the governments of New South Wales, Queensland, Tasmania, Victoria, Western Australian, and the Northern Territory.

In July 2017 our parent company in the United States, Equifax Inc, suffered a significant cyber security incident that led to a breach of data due to malicious hacker activity. Fortunately Equifax's Australian and New Zealand business was not part of the incident, and our systems were not compromised.

We have challenged ourselves to take the opportunity the breach provided us to turn our security program into an industry-leader, and we've set down that path. Equifax is investing \$200 million globally in incremental and accelerated IT and security spend in 2018 alone.

Equifax understands that the collection of consumer information carries with it an enormous responsibility to protect it. Data protection is a core part of our mission – it receives the highest level of priority at the executive and board levels, and throughout the entire organization.

INTERPRETATION OF THE PURPOSE TEST IS KEY

The *Public Data Policy Statement* has positioned open data for Government as the default position. Beyond reasonable exemptions for issues such as national security, Equifax supports this position. We note the twin controls that are built into data release considerations, namely the purpose test, and the five safes framework.

Guidance from the NDC in relation to the application of the purpose test will be key.

As identified above, Equifax is a significant consumer of Australian government data. We also supply government with a range of data-driven solutions. Equifax undertakes a range of activities with government that support the smooth functioning of the Australian economy. We play an important role as an intermediary between government and our customers, and as partner in ensuring the efficient delivery of government services.

Equifax recommends that the National Data Commissioner consider a broad interpretation in considering guidance in relation to the purpose test.

WE KNOW THE FIVE SAFES FRAMEWORK

Equifax notes the proposal to implement the *five-safes* framework as the second enforcement line in the draft release arrangements. Equifax has some familiarity with the five-safes through our business operations. We support the application of the *five-safes* as an appropriate second line review mechanism, and do not propose either amendments or additions to the *five-safes*.

We specifically note the comments in the issues paper:

Depending on the type and the sensitivity of the data to be shared, different controls or 'safes' will need to be applied at different levels. For example, if the data is less sensitive, it can be released to a broad range of users for a variety of purposes with fewer controls applied. On the other hand, if the data is more sensitive, or identifies individuals or businesses, the 'safes' need to be stringently applied, for example by data only being made available to authorised researchers in a secure access facility for specific purposes.

The Five-Safes framework further recognises that modifying the relevant data itself is only one way to manage re-identification risk, as applying controls across the environment where the data is provided can also be very effective in controlling the risk of re-identification. For example, agencies may be able to provide access to sensitive data in a secure environment, such as virtual laboratories with controlled outputs to manage this risk.

Much of the uses that Equifax applies to data requires its use in an identifiable fashion, or in a fashion to support our identification products. Therefore it is key that the interpretation of the *five-safes* is in line with best practice – namely that the application applies as a totality across the *five-safes*. The accreditation processes proposed in the data sharing system should account for the safe people requirements. Equifax's environmental arrangements will meet the safe setting requirements. The safe project requirements should form part of the purpose test.

In relation to both safe data and safe outputs – as they pertain to identity only – much of the work Equifax does requires identifiable data. We take our deidentification

obligations seriously, are confident that we can continue to meet the *five-safes* requirements as proposed in the Issues Paper.

OPENING UP PUBLIC DATA

There is an almost unlimited scope of data collected and stored by the Australian Government. There are a number of legitimate concerns that have historically held back data owners from board release, and whilst it is commendable to empower public sector data owners – data custodians – to allow them to hold back the release of data, it is important to acknowledge that any underlying concerns about the release of data may take some time to be resolved.

We support broad access to data – and are encouraged by the process proposed in the Issues Paper. For example, Equifax has sought access to the Australian and New Zealand Standard Industrial Classification (ANZSIC) Codes for some time – and a shift in policy towards releasing this data – and other non-sensitive data – makes good public policy sense. We have also sought access to a range of Australian Taxation Office data – such as employer or employment data, to support our identity and fraud solutions.

We also support the retention of existing data supply arrangements, as noted in the Issues Paper. As a commercial enterprise, we have invested heavily in the development of our data expertise to supply our customers, both public and private, with leading edge analytics and solutions. We have invested heavily in opening up data sources – often in partnership with government. We recommend that these existing data supply arrangements should be retained where appropriate, noting investments that may have been made to facilitate those arrangements.

THE DATA SHARING SYSTEM

Equifax supports the proposed data sharing system in the Issues Paper. We note that the proposed system is broadly in line with the system proposed in the Productivity Commission’s Data Availability and Use final report¹.

Equifax notes that the proposed data sharing system will comprise three key roles within the data system – Data custodians, Accredited Data Authorities, and Trusted users. Data custodians are Commonwealth entities and Commonwealth companies who collect data for any purpose.

The Issues Paper has sought input into matters relating to Accredited Data Authorities (ADAs), and Trusted users. Equifax notes that the Issues Paper does not specifically state that ADAs must be Commonwealth entities and/or Commonwealth companies. Equifax has a long history as a leading Australian entity with experience in data curation, collation, linkage, de-identification, sharing and release. For example, we were the first signatory to the Principles of Reciprocity and Data Exchange – the industry-developed data sharing framework for credit reporting data in Australia.

¹ <https://www.pc.gov.au/inquiries/completed/data-access/report>

We support the option of private companies playing the role of an ADA in the data sharing system – provided for example those entities are not then precluded from participating as Trusted users. Equifax already operates as a participant in safe environment data sharing arrangements both in Australia as a participant in other markets. We think it is prudent to allow the National Data Custodian to set framework questions, such as how the accreditation framework will operate. In line with the stated objectives in the Issues Paper for the proposed legislation, it is critical that the legislation is principles-based. By drafting the accreditation arrangements in a principles-based fashion, that will give the NDC the maximum capacity to respond to the fast-moving evolution of critical components of the accreditation framework, such as data security requirements and auditing arrangements. Consideration should be given to ensuring accreditation arrangements can be met as far as possible in partnership with requirements or standards already in place. Equifax recommends that the National Data Commissioner work with the Digital Transformation Agency to streamline accreditation requirements and ensure portability of assurance arrangements across the Australian Government.

THE NATIONAL DATA COMMISSIONER

The National Data Commissioner (NDC) will play a key role in ensuring the data sharing and release framework operates as desired. The Issues Paper has sought feedback on the powers that the NDC should have. Whilst a clear and considered view on the powers of the NDC is important, more than the regulatory powers, the collaborative culture that the NDC can support will be key.

Equifax supports broad compliance powers for the NDC, similar to those for the Australian Information Commissioner. It is important to consider who the regulated population is for the NDC, and then the behavior objectives that the regulation is seeking to achieve. Defining the regulated population for the NDC will be key, government entity and/or Commonwealth company, trusted users or end users, or technology providers, and so on. The proposed list of guidance topics suggests clearly that the NDC is intended to regulate Data custodians, Accredited Data Authorities, and Trusted users. It is less clear how the regulatory arrangements will work for suppliers or associated entities.

We are a partner to various governments across Australia – and clear guidance from the NDC will be key to ensuring an effective regulatory approach that does not overly complicate relationships and arrangements that may have previously functioned for years without the oversight of this new regulator. We recommend that the National Data Commissioner develop guidance to clarify regulatory arrangements where these partnerships between public and private stakeholders may complicate regulatory arrangements for the NDC.

RECOMMENDATIONS

Equifax proposes several recommendations for consideration in the further development of the Data Sharing and Release Legislation:

- The National Data Commissioner should take a broad interpretation of the purpose test in guidance for the new arrangements.

- The National Data Commissioner should ensure that the interpretation of the *five-safes* is in line with best practice and allow consideration of the five-safes as a totality when considering data release.
- Existing data supply arrangements should be retained where appropriate noting investments that may have been made to facilitate those arrangements.
- The National Data Commissioner should develop guidance over which entities are eligible to become Accredited Data Authorities (ADAs), and accreditation arrangements for both ADAs and trusted users.
- The National Data Commissioner should work with the Digital Transformation Agency to streamline accreditation requirements and ensure portability of assurance arrangements across the Australian Government.
- The National Data Commissioner should develop guidance to clarify the application of the regulatory framework where partnerships between public and private stakeholders may complicate regulatory arrangements.