Atlassian's Submission to the Department of Home Affairs in relation to the National Data Security Action Plan

Department of Home Affairs
datasecurityandstrategy@homeaffairs.gov.au

24 June 2022

We appreciate this opportunity to provide our feedback on the Discussion Paper published by the Department of Home Affairs on 6 April 2022 (the **Discussion Paper**) in relation to the National Data Security Action Plan (the **Action Plan**).

At Atlassian, we build enterprise software products to help teams around the world collaborate, including for software development, project management and content management. Our customers, and their teams operating all over the world, are at the heart of everything we do. This means that we understand the importance of data security in ensuring the trustworthiness of our own products and services.

We also understand that this is not just an issue for one company, one sector or one country. Our entire economy is increasingly digitised, highly interconnected (including globally) and strategically targeted by malicious actors, trends that have only accelerated in recent times. In addition to broader cyber security initiatives and efforts, Atlassian strongly supports efforts that seek to uplift data security capability and encourage better data security practices across the economy and across borders.

Atlassian welcomes this consultation process and appreciates the intent of the Discussion Paper and corresponding Action Plan to set forth a coordinated, proportionate and whole-of-economy approach to data security. As the Discussion Paper also acknowledges, the Action Plan will be set forth in an environment of — and need to take account of — the many existing and proposed domestic and international initiatives and policy settings seeking to address many of the same complex issues, including in related areas such as cyber security, privacy and data protection, and critical infrastructure.

Given this current landscape, we therefore strongly believe that the Action Plan should be guided and supported not only by the core pillars (secure, accountable and controlled) set forth in the Discussion Paper, but through key guiding principles that can help to drive the Action Plan towards clear, consistent and internationally-aligned standards, expectations and guidance.

Our approach and key principles

In late 2020, Atlassian published eight Principles for Sound Tech Policy,[1] which are attached to this submission. These Principles are intended to not only guide Atlassian's own engagement on important matters of public policy, but to set forth guiding principles for what we believe sound technology-related public policy should look like more broadly.

In line with those Principles, we believe that the Action Plan should:

- *acknowledge that tech (and trust) is global* — seize this opportunity to establish and maintain alignment with emerging international processes and regimes, including

[1] These Principles are also available for download at https://www.atlassian.com/blog/technology/regulating-technology.

through cross-certification and recognition of international standards and through the dissolution of ineffective barriers to interoperability (such as data localisation proposals);

- *define the playing field* and *treat the ailment, don't kill the patient* — consider and assess measures to uplift data security in a holistic and consistent manner, having regard to overlaps and intersections with related measures and policy settings; and
- *build the foundation for shared success* — seek to understand and take into account how organisations operate, interact with other businesses, governments and individuals, and secure their data in today's and tomorrow's digital and global economy, and target reforms to ensure that they will be effective within that context.

We accordingly strongly believe that the best outcomes will be achieved through an Action Plan that drives towards **coordinated**, **interoperable** and **effective** expectations and standards.

Our more specific comments on how key areas of the Discussion Paper can align with these objectives are set out below.

Coordinated

The Discussion Paper outlines the ways in which data security issues may intersect closely with other regulatory or legal issues, may arise in specific sectors or contexts (or economy-wide), and are likely to have global dimensions and impacts. In light of this multi-dimensional nature of these issues and as noted in the Discussion Paper, the need for coordination in the implementation of the Action Plan will be critical.

We therefore believe that the Action Plan should be situated within an overall digital regulatory and governance framework that applies across our digital economy, rather than considering the Action Plan in isolation or with a subject matter-specific lens. In the context of the use and management of Australia's data and information assets (including the security and protection of such data), this framework would be:

- governed by core principles, which would set forth a consistent, scalable and risk-based framework for all stakeholders that seeks to maximise the value of Australia's data assets and minimise the risk of misuse (for example, due to breaches or weaknesses in security or data protection), and inform the formulation and implementation of specific measures and tools within that framework;
- operationalised through one or more central 'clearinghouses', which allows government to build expertise (as to how technology operates, how data and information assets are used and managed, the opportunities and challenges this creates and how best to respond) and connections with industry, in a manner that can be accessed by a range of government agencies and regulators with responsibility across various sectors and subject matter areas; and
- supported by targeted and objective governance measures, guidance and tools (such as the Action Plan itself) that impose new or additional requirements on data use and management, which respond clearly to identified issues in a manner that aligns to and has the benefit of the overarching principles and institutional expertise.

This framework should be the key driver of an overall, comprehensive national approach to the use and management of data and information assets, as envisaged in the Australian Data Strategy, which seeks to realise the economic and societal opportunities that can arise from such use and minimise the corresponding harms and risks of misuse. As the Australian Data Strategy noted, data security is only one aspect of this multi-faceted framework and should be carefully considered and situated within it.

In our view, this proposed model is best able to ensure that the Action Plan can respond appropriately to the multi-dimensional nature of many of the issues involved, and achieve the principles-informed approach to data security set forth in the Discussion Paper.[2]

Interoperable

As mentioned in our submissions to earlier consultations in respect of privacy and cyber security,[3] many companies operating globally are subject to a wide array of standards, recommendations and obligations with respect to securing and handling data, including those under the EU's General Data Protection Regulation (among others). In our experience, this proliferation of standards can cause significant issues for businesses in understanding how best to effectively implement security risk management in their organisations in a way that aligns with the complex landscape of their own requirements, industry best practices and global compliance obligations.

An approach to data security that has regard to, and pursues, alignment with emerging international processes and regimes would not only contribute to supporting and improving Australia's (and Australians') overall data security posture. It will also lower global barriers to entry for Australian companies that are, or are seeking to be, export-ready, as well as benefiting Australian consumers who would have access to a wider variety of secure solutions from both local and international companies.

Effective

As the Discussion Paper acknowledges, the Action Plan can play an important role in improving and uplifting the guidance provided to businesses of all sizes with respect to data security processes, practices and tools. The complexity, scalability of risks and proliferation of available data security guidance means that there is a real opportunity to provide much-needed guidance to businesses on where and how to focus their data security efforts.

In our view and based on the considerations outlined in this submission above, this is likely to be best achieved through a multi-faceted approach to such guidance, including:

- the promotion of clear and actionable standards, guidance and best practice, which are either based upon existing global standards in this area (such as the ISO 27000 series) or mapped to such standards, and which have regard to the scalable and context-specific nature of data security risks within and across different sectors and industries;
- explicit consideration of how these standards can evolve over time, and how they currently and will in future align to equivalent guidance and processes in other countries (including those published by NIST, the UK NCSC, the Cloud Security Alliance and Center for Internet Security); and
- detailed education and training campaigns in support of any standards, guidance and related measures, in order to guide and influence companies in adopting these standards.

However, it is critical that any resulting measures, standards and guidance are both *actionable* and *effective*, by reference to the core pillars of the Action Plan and the overall outcome of improving data security across Australia. This means that the pursuit of such internationally aligned standards and guidance will need to be accompanied by a careful assessment of whether measures that purport to achieve these goals are in fact capable of doing so, or whether they can indeed serve to distract from this goal. For example, data localisation measures can often serve important functions — as the Discussion Paper notes,

[2] In addition, other similar models targeted at this form of regulatory coordination, such as the Tech Policy Design Centre's proposed Tech Policy and Regulation Coordination Model (available at https://www.anu.edu.au/research/research-initiatives/tech-policy-design-centre/publications), would also assist in achieving these aims.

[3] See https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988 and https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/atlassian.pdf.

they may facilitate audit compliance or clarify the jurisdiction(s) in which data is held for legal and compliance reasons — but these functions are often not, at face value, relevant to the security of that data. Indeed, data localisation can prevent companies from making decisions that that could promote data security (as well as access and reliability), including technical measures such as sharding or even the selection of an external service provider with an objectively stronger cyber security posture than an on-premise server or data centre.

Finally, it is important to acknowledge the crucial role that the Australian Government will be able to play in promoting these standards domestically, regionally and globally. This includes:

- role modelling of best practices for data security and data governance within and across all levels of Government; and
- collaborating with strategic partners in the Indo-Pacific and alliances such as AUKUS and the Quad, as well as multilateral global forums including the OECD, through contributing to and advocating for standards development processes, promoting regulatory interoperability, and sharing information on best practice recommendations.

Atlassian would be pleased to discuss these comments with the Department of Home Affairs, and is committed to working with the Government and other stakeholders to promote and uplift data security across our economy.

Yours sincerely,

David Masters
Head of Global Policy & Regulatory Affairs
Atlassian

Anna Jaffe
Director of Regulatory Affairs & Ethics
Atlassian

Atlassian
Public Policy

Atlassian Principles for Sound Tech Policy

Table of Contents

Atlassian Principles for Sound Tech Policy

Preamble

We at Atlassian are strong believers that the future of human endeavour and economic prosperity will increasingly flow from innovation and technology. And as 2020 has shown us, ever-greater digitisation is not only tomorrow's trend, but also today's urgent requirement.

But the pace of technology development means that all of us – individuals, private industry and government – must together develop policy frameworks that unleash the positive potential of technology for society while reducing any negative effects.

We know that developing a sound policy framework requires carefully considering the interests and rights of all vested stakeholders, as well as the potential impacts on them. This complex undertaking requires dedicated planning and process--as well as guardrails for the ultimate result. It is not surprising then that sometimes such policy efforts come up short of their intended aims.

This is why we think it is time for a reset on the conversation around tech regulation--one that fully encompasses the positive contributions of the tech sector to society, the legitimate regulatory requirements of government and protection of individual rights, as well as the need for a consistent and reliable environment for shared economic prosperity.

To contribute to this renewed conversation, Atlassian offers the following set of guiding principles to help government, industry, and the public converge on the essential qualities of sound regulation in the technology sector. If implemented, we believe that these guiding principles will result in targeted and proportionate policies, informed by a collaborative process, that ultimately unleash the positive potential of technology while fully addressing individual and societal interests – a true "win win" outcome for all of our communities.

Lastly, as these Principles make clear, we believe that collaboration is key to sound tech policy. As part of our drafting process, we engaged with numerous members of the tech sector, industry associations, and civic organizations who share our common vision. But to ensure that collaboration and improvement can continue even after publication, we are licensing these Principles under a **Creative Commons** license, so that others can adopt, modify and build upon these ideas as the dialogue continues.

Atlassian Principles for **Sound Tech Policy**

I. Define the playing field

Sound tech policy should have clear objectives. This means that everyone should be able to understand the specific problems that regulation seeks to solve, or the interests it seeks to support. More importantly, the regulatory solution should be clearly targeted at that identified problem. Unclear intent breeds distrust and concern.

II. Engage with the issue, don't dumb it down

Sound tech policy should be developed with a clear understanding of the relevant technology. Lawmakers and regulators may not all be technical experts, but if they engage with these experts and other stakeholders to understand the relevant technology and business models, they will be better positioned to respond to them through regulatory means. This can assist in identifying which regulatory means can be used effectively, and which ones are impractical or overly burdensome.

III. Treat the ailment, don't kill the patient

Sound tech policy should be proportionate, and should always seek to minimise unintended consequences. If regulatory responses are not properly considered and tested, they can overreach or lead to unintended and undesirable consequences. These consequences can be just as devastating to companies and their users as failing to act at all. Regulations should be surgical; government should not use a regulatory hammer where a scalpel is appropriate for its goals.

IV. Consult early, consult openly

Sound tech policy should be developed through open, consultative processes. When all relevant stakeholders are engaged early in regulatory processes, potential risks and unintended consequences can be identified and addressed before decisions are made. Open engagement also fosters greater trust in regulatory processes and creates space for both sides to clearly state their objectives or concerns. Early and extensive consultation is an obvious way to try to mitigate against a lack of understanding of the relevant technology or the business model of companies, and the consumer use cases. It also helps governments to ensure that regulations are as effective as possible.

V. Let the light in

Nothing is more uncertain than "black box" exercise of government discretion outside of the public eye. Sound tech policy should provide for transparency in government decision-making and set forth fair procedures that allow meaningful challenge of and detailed inquiry into those decisions.

VI. Address behaviour, don't punish success

Sound tech policy should seek to mold and target behaviours across a sector or drive outcomes on a systemic basis. It should not target specific individuals or companies. An approach that singles out individual organisations does not take into account the diversity and dynamism of the tech sector. More importantly, such an approach is not a sound long term approach addressing future challenges. This does not stop laws from ultimately being enforced in relation to identified individuals or entities, but regulations should not be made out against them specifically in the first place.

VII. Tech (and trust) is global

Sound tech policy should be coherent and consistent, mindful of global standards and able to enhance global interoperability. Local conditions must of course be considered, ensuring that any regulation forms part of a coherent local landscape. However, if competing regulatory frameworks are not also considered, there is a high risk that technology regulation will develop in a piecemeal manner that increases the burden on innovation, business, and consumers alike.

VIII. Build the foundation for shared success

Sound tech policy should provide a consistent and reliable framework for business and investment. We fully appreciate and support governments' legitimate interest in meeting regulatory goals and protecting consumers and the public, and the responsibility that all businesses share to ensure that this is achieved. It is equally important that the legislative process and outcome should be measured, fair, and reliable, in a manner that provides business stakeholders with the confidence to grow and invest in jobs, infrastructure, and improved products and services for their customers.