Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D22/11678

22 June 2022

Digital and Technology Policy Division
Department of Home Affairs

Online submission

Submission in response to National Data Security Action Plan discussion paper

Thank you for the opportunity to make a submission in response to the National Data Security Action Plan discussion paper (**discussion paper**).

The Office of the Victorian Information Commissioner (**OVIC**) has a unique regulatory focus, with combined oversight of privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic).

As the only jurisdiction in Australia with legislated information security standards, OVIC is at the forefront of information security regulation in Australia. Since 2014, OVIC has been responsible for setting the Victorian Protective Data Security Standards (**Victorian Standards**), and monitoring and assuring the security of public sector information and information systems (data systems) against the Standards, under the Victorian Protective Data Security Framework (**Victorian Framework**). Part 4 of the PDP Act provides authority for developing the Victorian Framework and setting the Victorian Standards. Over 3,000 Victorian public sector organisations are bound by Part 4 of the PDP Act.

OVIC understands the purpose of the National Data Security Action Plan (**Action Plan**) will be to:

- clearly articulate data security settings and requirements for governments, businesses and individuals;
- ensure a consistent approach to data security across federal, state, territory and local governments and industry; and
- uplift data security practices across governments, businesses, and individuals.[1]

The discussion paper is seeking views on how these purposes will be fulfilled in the Action Plan and suggests that a combination of new measures and existing legislative and policy mechanisms may be used.[2]

This submission provides OVIC's views on the development of the Action Plan and responds directly to questions 2, 3, 6, 7, 10-12, 14 and 15 of the discussion paper.

[1] Discussion paper, pages 6 and 14.
[2] Discussion paper, page 14.

Resourcing and planning will be crucial to the success of the Action Plan

1. OVIC supports the Action Plan's wide-reaching goals. They are admirable, and necessary, but will also be very challenging to achieve.

2. The Action Plan's target audience is considerably larger than OVIC's, and more diverse, covering all levels of government, industry, and individuals, not just the Victorian public sector. OVIC expends considerable effort to reach the upwards of 3,000 Victorian public sector organisations regulated under Part 4 of the PDP Act. Given its broader remit, the Action Plan is sure to face even greater challenges.

3. For this reason, providing appropriate resources to communications, monitoring, and assurance, to reach the wide array of stakeholders covered by the Action Plan, will be important if the goals of the plan are to be attained. Government incentives may also be required, to increase the numbers of data and information security professionals working in the public and private sectors. Without these measures, there is unlikely to be sufficient capability and resources to successfully uplift data security practices across the economy.[3]

Fulfilling the Action Plan's purpose to clearly articulate data security settings and requirements for governments, businesses, and individuals

4. OVIC strongly supports the Action Plan's intention to clearly articulate data security settings and requirements for individuals, industry, and all levels of government within Australia's federation. In OVIC's view, reducing duplication of effort wherever possible, and clarifying the data security landscape, the language used and the scope of coverage, will be essential to achieving this goal.

Clarifying the landscape

5. The information security landscape has become increasingly complex in recent years due to:

    - The existence of many distinct and overlapping requirements contained in legislation, regulation, frameworks, strategies, plans and other soft-law guidance and administration (**requirements**) at federal, state and local government levels. There is no clear hierarchy of requirements, and many requirements contain complex exemption criteria that is not easily understood. This environment makes it hard for such a wide variety of stakeholders to understand what law and guidance applies to them.

    - Inconsistency in the coverage of various requirements. This makes it hard for stakeholders to understand what type or form of information and information systems each requirement applies to, and where requirements overlap.

    - Inconsistency in framing and use of terms and supporting definitions in intersecting or overlapping requirements. Where there is a distinct need to use the same term but with different meanings, this should be made clear to stakeholders to avoid confusion. For example, 'aggregation' in a security sense and 'aggregation' in a statistical sense.

    - Inconsistency in the approach taken to securing information. This makes it hard for stakeholders to understand how they should securely manage the information they handle and the systems they use. For example, there are different approaches to classifying the security value of information and different risk-based and compliance-based approaches to implementing security controls.

[3] Mark Eggleton, 'Cybersecurity desperate for people power', *Australian Financial Review* (online, 25 May 2022) https://www.afr.com/technology/cybersecurity-desperate-for-people-power-20220522-p5anja.

6. At present, OVIC's information security unit spends considerable time discussing the applicability of various state and federal requirements with its stakeholders. If requirements were clear, OVIC would have more time available to it, to provide practical security advice to stakeholders, to help uplift information security practices across the Victorian public sector.

7. To improve clarity of requirements, OVIC recommends the Action Plan contain a clear visual layout and explanation of:

    - the hierarchy of requirements and how they interact and intersect, including the crossover of requirements at federal, state, territory and local government level;
    - the problem each requirement tries to solve (why it exists);
    - what information each requirement applies to (type, form and security value);
    - who each requirement applies to (which stakeholders); and
    - how it applies to each stakeholder, including a clear outline of roles and responsibilities. For example, in the form of a *Responsible, Accountable, Consulted* and *Informed* (**RACI**) table.

Clarifying language and definitions

8. OVIC agrees with the discussion paper that "[a]greeing on key data security terms and concepts is fundamental to addressing confusion, misunderstandings and establishing clarity" across all jurisdictions in Australia.[4]

9. OVIC notes the discussion paper:

    - defines 'data' broadly, to include non-digital information, then limits the definition of 'data security' to digital information and digital systems and networks only;[5]
    - distinguishes between 'data security' and 'cyber security':

        > "**Data security** refers to protecting the information collected, processed, and stored on digital systems and networks.
        >
        > This is distinct to the related concept of **cyber security**, which encompasses measures to protect the confidentiality, integrity, and availability of systems, devices, and the information residing on them."[6]

    - uses the phrase 'all data types' when explaining the difference between privacy and data security: "Data security seeks to address unauthorised access to all data types".[7]
        - In OVIC's view, the language "all data types" could be construed by some stakeholders to include hard copy and verbal data types, as well as digital. If the intention is to limit the scope of the Action Plan to soft copy information and ICT systems only, the language used to convey this will need to be carefully considered and clear.

10. In contrast to the discussion paper, in Victoria:

    - the Victorian Framework and Standards, developed by OVIC under Part 4 of the PDP Act, do not limit security requirements to the protection of information on "digital systems and networks"

[4] Discussion paper, page 18.
[5] Discussion paper, definitions page.
[6] Discussion paper, pages 18 and 19.
[7] Discussion paper, definitions page.

only. The PDP Act regulates *all forms* of public sector information and information systems – digital, hardcopy and verbal.

- OVIC does not consider it necessary to distinguish between the terms 'data security' and 'cyber security' when it comes to protecting information. The Victorian Framework and Standards protect public sector information from a range of security threats, not just the threat of unauthorised access.

- OVIC's regulatory framework uses a combination of risk-based security measures spanning each of the protective security domains (governance, information, personnel, information communications technology (**ICT**) and physical security) to maintain (protect) the confidentiality, integrity and availability (**CIA**) of public sector information assets and systems. The CIA triad is widely recognised as representing traditional information security attributes. They are not a concept exclusive to cyber security, as the discussion paper suggests. For example, the Information Security Manual produced by the Australian Cyber Security Centre uses the CIA triad in its definitions of both 'data security' and 'cyber security'.[8] The discussion paper's focus on protecting data from unauthorised access emphasises potential compromises to the confidentiality of the information or information system but does not afford the same emphasis on maintaining the integrity and availability of the same information and systems. In OVIC's view, the full CIA triad needs to be represented for there to be a holistic approach to the protection of information and information systems.

- OVIC uses the term 'information security', which is not used in the discussion paper. Whilst the PDP Act uses the term 'data protection', this is not an accurate description of the subject matter that is regulated under Part 4 of the PDP Act.[9] To overcome the misleading words used in the PDP Act, and to clarify the subject matter that is regulated under Part 4 of the PDP Act, OVIC uses the term 'information security' in its guidance and messaging (other than when specifically referring to the legislation), to ensure that stakeholders are not misled into thinking they only need to protect soft copy (digital) information and/or information systems, or personal information only. OVIC recognises that information presents in many different formats, not just digital, and represents a safety and security risk when the confidentiality, integrity and/or availability of verbal or hardcopy material, or non-personal information, is not adequately protected.

11. Whichever phrase is ultimately adopted by the Action Plan ('information security', 'data security' or something else), OVIC strongly recommends the Action Plan, and any intersecting legislation, administration and policy initiatives sitting under its umbrella, adopt a clear and common understanding of:

    - the forms and types of information that are intended to be protected by the phrase; and

    - the protective security domains intended to be covered by the Action Plan.

12. The scope of the Action Plan needs to be crystal clear. For example, if the intention is to only protect digital information and systems, and only focus on the ICT protective security domain, this should be made explicit in the Action Plan. Stakeholders should be able to easily understand if the Action Plan does not protect all information and information systems and does not focus on all protective security domains across the full CIA triad. If the intention of the Action Plan is to *not* offer a holistic approach to

[8] Australian Cyber Security Centre, 'Cyber Security Terminology', Information Security Manual (ISM) https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-terminology.

[9] 'Data protection' is used to refer to privacy and personal information in some settings, such as the European Union's General Data Protection Regulation. The word 'data' can also be understood in a limiting way, as electronic information only. In contrast, Part 4 of the PDP Act regulates all types and forms of public sector information.

the protection of information and information systems, or to *not* work towards a holistic approach in stages, this should be explained in the Action Plan.

13. In OVIC's view, it would be preferable for the Action Plan to encompass information security in the broader sense, capturing all forms of information – both digital and non-digital, and utilising all protective security domains to maintain the CIA triad.[10] OVIC understands the Action Plan is informed by the Digital Economy Strategy,[11] which may limit a broader remit. However, a siloed focus on electronic information, or personal information, has the potential to expose Australia to harm or damage that could be avoided if a more holistic approach to information security is adopted.

Reducing duplication of effort between data security and cyber security policy initiatives

14. In August 2021, OVIC provided a submission[12] to the *Strengthening Australia's cyber security regulations and incentives* discussion paper (**cyber security discussion paper**)[13] which seeks to progress policy initiatives under Australia's Cyber Security Strategy 2020. OVIC understands the federal government is developing this Action Plan at the same time as progressing policy initiatives arising from the cyber security discussion paper, and that the National Data Security Action Plan is intended to sit alongside Australia's Cyber Security Strategy 2020.[14]

15. To improve clarity and consistency, and avoid duplication of effort, OVIC recommends the federal government's cyber security policy initiatives sit underneath, not alongside, the Action Plan.[15] That is, OVIC recommends a hierarchical approach is taken, rather than viewing data security and cyber security as separate, complementary requirements.

16. In Victoria, the Victorian Framework and Standards, developed by OVIC under Part 4 of the PDP Act, underpin Victorian Government initiatives involving the security of information and information systems, including those that specifically cater to cyber security. The Cyber Security Branch within Digital Victoria adopts the Standards issued by OVIC, and in turn assists agencies and bodies in their application of the Standards. The Victorian Cyber Strategy aligns with and refers to the Victorian Framework and Standards.[16] Victoria's approach ensures stakeholders are presented with harmonised material and avoids duplication of effort.

17. As recommended by OVIC in response to the cyber security discussion paper,[17] the federal government may wish to consider legislating information security requirements more broadly as part of the Action Plan. All initiatives at the federal level and within the private sector that involve the protection of information would then be subject to the same legislated requirements.

18. Legislating 'information security' recognises that data security (or cyber security as framed in the Action Plan) is only one facet of good information security risk management, and broadens legislative protections to cover digital and non-digital information and systems. By providing a legislative base to

[10] The definition of 'data' in the discussion paper is wide enough to include all forms of information.
[11] Discussion paper, page 15.
[12] OVIC submission to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, August 2021, https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/office-of-victorian-information-commissioner.pdf.
[13] Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's Cyber Security Strategy 2020* (August 2021) https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives.
[14] Discussion paper, page 14.
[15] See the recommendation made in OVIC's submission to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, August 2021, [13]-[18] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/office-of-victorian-information-commissioner.pdf.
[16] See Victorian Government, 'Victoria's Cyber Strategy 2021: Mission Delivery Plans 2021-2022', available at https://www.vic.gov.au/victorias-cyber-strategy-2021-introduction#download-the-pdfs.
[17] See the recommendation made in OVIC's submission to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, August 2021, [13]-[18] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/office-of-victorian-information-commissioner.pdf.

this program of work, a common language and approach could be formally established, improving clarity and consistency for stakeholders, and reducing duplication of effort.

Fulfilling the Action Plan's purpose to ensure a consistent approach to data security across federal, state and territory governments and industry

Response to question 6 – How can data security policy be better harmonised across all jurisdictions?

19. In OVIC's view, data security policy could be better harmonised across jurisdictions through:

- consistent use of terms;
- consistent definitions underpinning consistent terms;
- widening the focus from ICT only,[18] to a more holistic view of information security that considers all forms of information (electronic, verbal and hardcopy material), all types of information (not just personal information), all protective security domains (not just cyber), and addresses all stages of the information and system lifecycle;[19]
- clearly identifying the complementary and competing legislation, regulation, soft-law guidance and administration materials that have a relationship to information security. This includes clearly articulating the specific forms and types of data or information that are in scope and clearly identifying who the legislation/regulation/soft-law guidance applies to and in what context;
- clearly articulating roles and responsibilities of government (including the various regulators and oversight bodies at the federal, state, territory, and local government levels), industry and the community. Expectations about who is expected to do what, when and where should be clear;
- establishing clear lines of accountability and oversight, including well-defined monitoring and assurance regimes at federal and state levels, with clear and serious penalties embedded to deter adverse actions;
- harmonising, where possible, legislative and regulatory requirements across jurisdictions. For example, Victoria is the only jurisdiction in Australia with legislated information security requirements overseen by a single regulator with combined responsibility for information security, privacy and freedom of information. Given the successful implementation of this model, OVIC recommends exploring a similar model for other jurisdictions;[20]
- harmonising classification processes used to assess the security value information (i.e. assessing the sensitivity or significance of particular information or system assets). Currently, most state and territory jurisdictions use versions of the Business Impact Levels (**BILs**) to inform the assessment of information and information systems. However, the descriptions, levels and impacts offered under each of these different jurisdictional BIL tables undermine consistency in this foundational activity. For example, the terminology 'National Interest' has the tendency to skew stakeholders' perception of levels across the BILs themselves. If this foundational assessment activity is harmonised, stakeholders across the nation will have greater confidence that information and systems they are accessing and using have been assessed in a largely consistent way. In turn, this would support the

[18] The discussion paper's definition of 'data security' is limited to digital information and systems: Discussion paper, definitions page.
[19] For example, the discussion paper's 'Accountable' pillar only references storage of data, not other aspects of the information lifecycle such as collection and disclosure: Discussion paper, page 17.
[20] See the recommendation made in OVIC's submission to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, August 2021, [13]-[23] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/office-of-victorian-information-commissioner.pdf.

subsequent application of commensurate controls (security measures), allowing for greater interoperability of systems and enhancing secure information sharing practices;

- identifying and investing in behavioural change to uplift information security knowledge and practices that may be lagging in some jurisdictions, industries or community groups more than others;

- recognising and addressing where different levels of risk appetite and tolerance exist across various jurisdictions, industries and community groups to understand where the challenges lie in achieving consistent adoption and uplift of information security controls;

- resourcing equitably, to ensure adequate capacity and capability exists across all jurisdictions, especially if a risk-based approach is preferred;

- harmonising the principles found in various requirements into one core set of principles used across all jurisdictions;

- mapping the Australian Data Strategy's 'three core pillars' onto existing frameworks, to help stakeholders understand their relevance in practice;[21]

- investigating and addressing pain points, to understand why some jurisdictions may be reluctant to implement certain controls. This research would lead to a better understanding of the risks posed to data and data systems, and allow for targeted investment decisions to support secure outcomes for everyone.

Response to question 2 – How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?

20. OVIC supports the intention to align Australia's data security framework with international standards, where it makes good sense to do so. Aligning Australia with international best practice would reduce regulatory burden on businesses operating in international markets and government agencies caught by laws of international jurisdictions. Minimising the overlapping application of international, national, and state based frameworks to the same data activities also clarifies obligations and reduces time spent by regulators in helping stakeholders understand which frameworks apply to them.

21. The example framework used in the discussion paper question raises questions about the intended scope and coverage of the Action Plan, given the data security components of the European Union's *General Data Protection Regulation* apply only to personal data, not data in a more general sense. OVIC recommends the Action Plan address the security of all types of information, not just personal information. If the intention is to address the security of personal information only, the Office of the Australian Information Commissioner (**OAIC**) should be closely consulted to ensure alignment of legislative requirements and reduce duplication of effort.

22. If the intention is to uplift information security practices for all types of information, not just personal information, Australia could look towards adopting international standards, such as those in the ISO/IEC 27000 series (for example, ISO/IEC 27001 and ISO/IEC 27002).[22] The federal government may also consider looking to mature frameworks such as the Centre for the Protection of National Infrastructure[23] and the National Institute of Standards and Technology,[24] to consider if concepts,

[21] For example, the "Control" pillar in the discussion paper does not clearly distinguish between issues directed at the public and issues directed at government or business: Discussion paper, page 17.
[22] See ISO, 'Popular Standards' available at https://www.iso.org/isoiec-27001-information-security.html.
[23] Centre for the Protection of National Infrastructure, United Kingdom, https://www.cpni.gov.uk/.
[24] National Institute of Standards and Technology, United States Department of Commerce, https://www.nist.gov/.

principles and approaches in these frameworks could be borrowed to inform the development of a holistic data security action plan for Australia.

23. Finally, OVIC draws attention to a new International Standard, ISO 22340: *Security and resilience – Protective security – Guidelines for an enterprise protective security architecture and framework,* due to be published later this year.[25] OVIC recommends the Action Plan consider ISO 22340, given it aligns with the federal government's Protective Security Policy Framework (**PSPF**) and will likely be adopted as an Australian standard. OVIC contributed to the development of ISO 22340 and would be pleased to provide further information to the government as the Action Plan progresses.

Response to question 3 – What additional guidance or support from Government would assist you to meet a principles-informed approach to data security?

24. Whether the Action Plan adopts legislated mandatory standards, a legislated risk-based framework or utilises policy guidance only, all options require the capacity and capability of government and industry to implement the Action Plan successfully.

25. The Australian National Audit Office recently found that despite the "Top Four" mitigation strategies being mandated under the PSPF, none of the seven major departments selected for audit had implemented these strategies fully and effectively.[26] This suggests that mandatory standards by themselves are insufficient to provide effective security. OVIC expends substantial effort to engage Victorian public sector organisations with education and information. This includes engagement officers assigned to various sectors, to ensure continuing and effective communication. The success of the Action Plan will depend upon sustained and capable personnel to assist agencies in meeting their commitments.

26. OVIC's experience in this area suggests the most critical factors for effective mitigation are executive buy-in, and a clear understanding of risk assessment and risk management.

27. Additional funding and strong oversight and assurance mechanisms will be necessary, to support the uplift of data security practices, and to properly monitor and manage how parties interact with and adopt the requirements of the Action Plan.

Response to question 7 – Who is currently responsible for ensuring consistent and commensurate uplift of local government data security and how can this be strengthened? Do you think responsibilities should be shared across more bodies, or shifted elsewhere entirely?

28. In Victoria, local government is responsible for ensuring the protection of its own assets, except in instances where a regulated entity under Part 4 of the PDP Act is nested within a local government authority (**LGA**). In practice, this accounts for all 79 LGA's in Victoria. In OVIC's experience, shared monitoring and oversight confuses stakeholders and duplicates efforts of regulators and administrators.

29. In OVIC's view it is preferable to avoid devolved or shared monitoring and oversight responsibilities at the state and local government levels. OVIC recommends additional resources be provided to one oversight agency at the state level, to regulate the information security practices of state and local government bodies.

[25] For a summary of the new standard see Matthew Curtis, 'Timely arrival of a new and much needed protective security standard', *Security Solutions* (online, 26 March 2022) https://www.securitysolutionsmedia.com/2022/03/26/timely-arrival-of-a-new-and-much-needed-protective-security-standard/.

[26] See: 'Cyber Security Strategies of Non-Corporate Commonwealth Entities', Auditor General Report No. 32 2020-21, p.9-10, at https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities

Response to questions 10 and 11 – How can the Australian Government further support business to understand the value of data and uplift its data security posture? Are there any limiting factors that would prevent Australian industry and businesses from effectively implementing an enhanced data security regime?

30. In OVIC's view, the most important education piece is to explain why a business should engage with and implement information security controls. If a business is not legally required to protect the data it processes and stores, it will likely have limited motivation to uplift its information security practices.[27]

31. Information security should be understood by business as a category of risk that requires managing, similar to occupational health and safety and financial risks. This approach moves information security out of compliance and into organisations' existing risk management frameworks. In OVIC's view embedding information security into business-as-usual risk activities is likely to get more traction within an organisation and produce long term cultural change and uplift of data security practices, than an approach motivated only by compliance.

32. Tangible and ongoing support to implement security controls will be necessary.[28]

Response to question 12 – Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).

33. In OVIC's view the size of the business is not the main criteria for determining the value of the information the business holds. A small business may hold quite sensitive or significant information and should be provided with guidance on how to identify or recognise this material, and in turn, how to keep that information safe. The content and context of the information should form part of the basis in assessing the security value of the business's material.

34. OVIC provided detailed views on the regulation of large, medium and small companies in its submission to the cyber security discussion paper.[29]

Response to question 14 – Does the Australian Government currently have sufficient public information for consumers and citizens on data security best practice? How can we make that information more easily accessible, usable and understandable?

35. To improve community awareness and understanding of information security practice in everyday life, the government may wish to consider:

    - TV, social media and public signage campaigns, to raise awareness of the issue;
    - incorporating visual, auditory and written content in public messaging;
    - using clear, practical examples of the consequences of poor information security practices.
    - using simple step by step videos that empower individuals to improve their information security habits;

[27] See cyber security discussion paper, chapter 2.
[28] For further information see OVIC's submission to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, August 2021, [34]-[37] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/office-of-victorian-information-commissioner.pdf
[29] See OVIC's submission to the *Strengthening Australia's cyber security regulations and incentives* discussion paper, August 2021, [24]-[35], [38]-[46] https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/office-of-victorian-information-commissioner.pdf

- using plain language to explain to the public where their data travels. For example, when using commonly available mobile applications and web browsers;

- providing enhanced and targeted education in schools, to ensure future generations understand how to keep information safe, and the importance of doing so; and

- providing targeted, clear, and succinct messaging to older generations who may be more likely to have high value assets and can be more easily exploited if information security and cyber safety is not well understood.

Response to question 15 – Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?

36. OVIC considers the notifiable data breach scheme administered by the OAIC under the *Privacy Act 1988* (Cth) (**Privacy Act**) to be an appropriate accountability mechanism. However, OVIC supports the OAIC's recommendation to enhance its enforcement powers under the Privacy Act, to enable the Information Commissioner to directly issue monetary fines for interferences with privacy (including data breaches), rather than first needing to apply to the court for a civil penalty order.[30]

37. In OVIC's view, empowering the Information Commissioner to issue monetary fines, similar to the United Kingdom's Information Commissioner's Office, will help to deter inappropriate practices and incentivise information security uplift across government and industry. This in turn, will improve public trust.

38. Other measures to improve public trust include:

    - Placing a greater emphasis on the transparency of information flows and the steps taken by governments and businesses to secure the public's information. Transparency improves trust and assists individuals to make more informed decisions about who to do business with, what information to share, and when.

    - Making it easier for an individual to request a public or private entity to delete the information it holds about that person. Deleting information also reduces the potential harms and security risks that can arise from a data breach.

Thank you again for the opportunity to contribute to the development of the National Data Security Action Plan. I have no objection to the Department of Home Affairs publishing this submission and will be publishing a copy on the OVIC website.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Emma Stephens, Senior Policy Officer, at Emma.Stephens@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner

[30] OAIC submission to Privacy Act Review Issues Paper [9.31]-[9.37] https://www.oaic.gov.au/privacy/the-privacy-act/review-of-the-privacy-act/privacy-act-review-issues-paper-submission/part-9.