Governance Institute of Australia

T +61 2 9223 5744 **F** +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

24 January 2021

Attorney-General's Department
3-5 National Circuit
Barton ACT 2600
By email: privacyactreview@ag.gov.au

Dear Sir / Madam,

Review of the Privacy and Online Privacy Bill Exposure Draft

Who we are

Governance Institute of Australia is a national membership association, advocating for our network of 43,000 governance and risk management professionals from the listed, unlisted, public, not-for-profit and charity sectors.

As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates and postgraduate study. Our mission is to drive better governance in all organisations, which will in turn create a stronger, better society.

Our members have primary responsibility for developing and implementing governance frameworks in public listed, unlisted and private companies, as well as not-for-profit organisations and the public sector. They have a thorough working knowledge of the operations of the markets and the needs of investors. We regularly contribute to the formation of public policy through our interactions with Treasury, ASIC, APRA, ACCC, ASX, ACNC and the ATO.

Our activities in this area

Governance Institute members have a strong interest in digital technology policy and take the governance and risk management of privacy, data protection and cyber security in all sectors very seriously. As a membership organisation, we have advocated for some time for digital transformation and modernisation in many areas of corporate regulation, including supporting virtual and hybrid AGMs, digital document execution, digital shareholder communications, and the introduction of Director Identification Numbers. Many of our members are working as governance and risk professionals in a range of organisations that are part of or connect with the digital economy, from the largest listed companies responsible for critical infrastructure to small businesses and not-for-profits. They are experienced in considering the industry and economy-wide implications of data and technology governance, cyber security, and digital transformation.

Governance Institute is a founding member of the ASX Corporate Governance Council, which produces the leading Australian statement on corporate governance, the Corporate Governance Principles and Recommendations. Recommendation 7.2 of the most recent edition explicitly acknowledges the importance of an organisation's risk management framework dealing adequately with privacy and data breaches, cyber security risks, and digital disruption.[1] We strongly supported this inclusion. While the Corporate Governance Principles and Recommendations are directed at listed entities, they influence the governance practices of Australian organisations of all types and in all sectors.

[1] ASX 2019, *Corporate Governance Principles and Recommendations 4th Edition*, p. 27.

We also produce a range of thought leadership and industry guidance in relevant areas. In recent years our Risk and Technology policy committee has published Good Governance Guides on the topics of cloud services, digital transformation, digital trust, technology strategy, technology governance, cyber security, data as an asset, and ethical use of artificial intelligence.

In recent weeks, Governance Institute published a report that identified data privacy and cyber security as two of the biggest challenges associated with technological disruption facing boards of directors into the future.[2] We published a report in 2020 that identified cyber security, artificial intelligence and digital disruption as key trends likely to impact on risk management professionals by 2025.[3] We also collaborated in 2020 with CSIRO Data61 to compile a report on digital trust that examined key privacy and consumer data issues.[4] We regularly contribute to a range of consultations on digital themes including Australia's 2020 Cyber Security Strategy and the Digital Australia Strategy 2030. Governance Institute also contributes to the international debate on digital technology and data governance issues in its capacity as a division of The Chartered Governance Institute (CGI), an international body with over 30,000 members worldwide.

Executive summary

- Governance Institute members welcome the opportunity to make this submission on the critical issue of privacy protections. We support the aims of the Government in working towards an enhanced privacy scheme that continues to protect consumers, keeps pace with rapid technological change, and promotes good governance and risk management in organisations.

- We consider that the current principles-based privacy framework and Notifiable Data Breach (NDB) scheme remains largely fit for purpose and should be retained, with opportunities for targeted enhancements that balance the compliance burden.

- We recommend that Government consider the potential unintended impacts of the introduction of direct action and tort of privacy.

- We recommend that the Government consult further on any proposal to remove or lower the $3 million annual turnover exemption, including with the not-for-profit sector.

- The adjustments to Australia's privacy scheme proposed in the Discussion Paper and the exposure draft legislation, taken as a whole, constitute a significant expansion of the scheme that would bring it into closer alignment, and in some areas go beyond, the European General Data Protection Regulation (GDPR), which is widely considered the most rigorous privacy regime globally. For this reason, we urge the Government to carefully consider and continue to consult with industry on these proposals and their practical impacts, especially the potential impacts on smaller organisations and not-for-profits.

- We broadly support enhanced enforcement powers, mechanisms and penalties for the regulator and the introduction of new individual rights to 'withdraw consent', request the erasure of personal information, and seek redress for interferences with privacy, provided these mechanisms are balanced against practical and commercial considerations.

- We strongly support the Discussion Paper's proposed reforms in the area of consent.

- We encourage all levels of government to coordinate to ensure better harmonisation between privacy, data breach, cyber security data sovereignty and critical infrastructure regulation.

[2] Governance Institute, 2021, *Future of the board*, p. 10.
[3] Governance Institute, 2020, *Future of the Risk Management Professional*, p. 19.
[4] Data61 and Governance Institute of Australia 2020, *Digital Trust: Corporate awareness and attitudes to consumer data*.

General comments

In developing this submission, Governance Institute has applied a broad sectoral lens reflective of our wide membership base. As an example, the primary industry sectors making notifications under the Privacy Act's NDB scheme are health service providers, finance, legal, accounting, management services, government, and insurance[5] – all of which are represented among our professional members. Rather than focussing on particular impacts in any one sector, our members have taken into account a range of considerations relevant to governance and risk management and the wider economy, in line with our vision of 'strengthening society through governance excellence'.[6] Given the expertise and areas of focus of our members, we have combined our comments on a select number of provisions in the Privacy Act Discussion Paper and the Online Privacy Bill Exposure Draft.

Governance Institute members observe that in recent years there has been a significant uplift in global privacy laws with a focus on greater transparency and individual control over data. This has been coupled with a greater focus on cyber security regulation and its interaction with the protection of sensitive personal information. Many regulatory responses have been prompted by the accelerated growth of digital technologies and large online platforms, both of which pose significant policy challenges. We note that the addition of the mandatory element of the NDB scheme to the Privacy Act in early 2018 and the final report from the Australian Competition and Consumer Commission (ACCC) the following year that urged 'holistic, dynamic reforms' to the Privacy Act were significant and positive steps in the ongoing improvement of the scheme.

We support the Commonwealth Government setting a clear direction for privacy law reform and considering an extensive range of reform options. It is important to maintain that momentum into legislation and implementation. Australian governments and regulators at the federal, state and territory level must continue to take a leading role to ensure regulatory frameworks remain capable of protecting consumers, keeping pace with rapid technological change, and promoting good governance and risk management in organisations. Rather than a once-off review, all levels of government should continually improve, maintain and, where possible, harmonise their legislative frameworks. Regulatory reviews every 18 months to two years are now probably required, due to the pace of regulatory and technological change.

Governance Institute recognises that privacy and data protection, strong cyber security and effective data governance are important components of the governance and risk management frameworks of most, if not all, organisations in the modern Australian economy and that these are closely interrelated areas of policy. We note with approval that both the Discussion Paper and previous submissions from the Office of the Australian Information Commissioner (OAIC) recognise the 'fundamental link between strong cyber protection and the protection of personal information'.[7]

As a starting point, our members do not believe there is a need for substantial material change to the Privacy Act's underlying principles-based approach and the NDB scheme. This is consistent with what is proposed in the Discussion Paper. They agree that the current principles-based approach has been effective in managing the regulatory compliance burden on regulated entities and that there is room to enhance the scheme without introducing an overly prescriptive regulatory approach.

The Discussion Paper and the explanatory memorandum of the exposure draft legislation devote significant space to addressing digital harms. Our members broadly agree, but would also stress

---

[5] Office of the Australian Information Commissioner (OAIC) 2021, 'Notifiable Data Breaches Report: January to June 2021', viewed 11 November, p. 1, https://www.oaic.gov.au/__data/assets/pdf_file/0013/2803/oaic-notifiable-data-breaches-report-jan-june-2021.pdf

[6] Governance Institute of Australia 2020, 'Strategic Plan 2020-2025', https://www.governanceinstitute.com.au/about-us/our-strategy/

[7] Discussion Paper, page 146

the opportunities and potential of digital technology. As noted above, Governance Institute has strongly supported digital modernisation reforms including virtual and hybrid AGMs, digital document execution, and digital shareholder communications. We believe there should also be a focus on the benefits of digital technology, not just on risks and harms. Our members consider it is vital that governments, academics, businesses and the community work collaboratively to promote the digital economy and Australia's digital future.

Finally, we welcome the Government's stated intention to minimise regulatory burden. It is important for this Privacy Act reform process to achieve a balance between strong consumer safeguards that keep pace with rapid technological and regulatory changes globally and a workable level of regulatory compliance burden. Governance Institute members have formed the view that the Discussion Paper proposes a substantial expansion of the existing privacy scheme that would bring it into closer alignment – and in some places go beyond – the GDPR in Europe, and members have expressed a range of views on the practical impacts of such an expansion. Some members take the view that significantly expanding the scheme's scope and application would have potential benefits. They include the potential to attain a GDPR decision of adequacy from the European Commission, the prevention of regulatory arbitrage, and ensuring the privacy protections available to Australians are consistent with those in other developed economies. Other members have expressed concerns about compliance costs, uneven impacts on smaller organisations, and the potential to stifle innovation. We believe this range of views illustrates the need for Government to proceed cautiously and strike an appropriate balance.

Specific responses

Informed consent and pro-privacy defaults

Governance Institute has previously argued that informed consent is 'vital to upholding contractual rights and mitigating risks to potential breaches of privacy, misuse of personal data and other dangers unique to the digital economy' and advocated for the need for terms and conditions to be more accessible.[8]

Governance Institute members note the ACCC's earlier comments on the 'privacy paradox', defined as the 'perceived discrepancy between the strong privacy concerns voiced by consumers who, paradoxically, do not appear to make choices that prioritise privacy'. Our members consider that Australians do generally care strongly about their privacy but are often incapable of giving effect to these concerns, often due to the complexity of terms and conditions used under the current consent model, which often lack clarity and precision. It is often impractical for consumers to opt out of using popular digital platforms and services despite any real and present concerns they may have over the use of their sensitive personal data.

We believe there is a role for government, under an enhanced privacy scheme, to better enable informed consent through clearer and more accessible terms and conditions, but there is also an opportunity to further protect consumers by acknowledging the limits of informed consent in this context. For these reasons, we agree there should not be an overreliance on notice and consent mechanisms.

Governance Institute recommends the Government moves forward with Discussion Paper proposals 8.1, 8.2, 8.3, 8.4, 9.1 and 9.2. **Governance Institute also recommends** that the Government consider enabling pro-privacy settings by default under Option 1 in proposal 12.1.

Definition of personal information

The proposed reforms significantly expand the definition of 'personal information'. While our members do not object to this expanded definition, they consider that care needs to be taken in drafting the legislation to ensure that there is clarity around what is in fact 'personal information', so that organisations have certainty around what types of information that they handle fall within this expanded definition. Confusion can arise if the concept is defined in a nebulous or ambiguous way.

[8] Governance Institute of Australia 2021, *Submission on Digital Australia Strategy 2030*, pp. 7-8.

Governance Institute recommends that care needs to be taken in drafting the legislation to ensure that there is clarity around what is in fact 'personal information'

OAIC's role in cyber security regulation

The Australian Privacy Principles currently recognise the importance of governance, risk management and culture to the protection of privacy. APP 11.1 and 11.8 currently require organisations to take active measures, including adopting governance, culture and training strategies, where relevant, to ensure the security of personal information they hold. This is appropriate, as Governance Institute is firmly of the view that cyber security and privacy protection go hand-in-hand as part of effective governance and risk management.

However, it is also important that Australia's cyber security regulatory frameworks are cohesive, regulatory overlap is avoided, and that enforcement activities are overseen by agencies with appropriate expertise and resourcing.

The Discussion Paper makes several proposals that touch on cyber security. It proposes that APP 11.1 could be amended to clarify that reasonable steps include 'both technical and organisational measures' and to include a list of factors, drawn from the current APP guidelines, that influence what reasonable steps may be required. According to the Discussion Paper, the Government is 'proposing to develop an APP code to specify minimum cybersecurity standards required by APP 11.1'.[9] The Discussion Paper also raises the prospect of the OAIC providing technical guidance for regulated entities and investigating alleged breaches of APP 11.1 'in relation to cyber security'.[10]

Governance Institute supports in principle the addition of further clarity to Principle 11. This is on the basis that it signals to organisations the critical importance of this principle and encourages organisations to continually improve their governance and risk management frameworks and cyber security posture. However, we would discourage Government from taking a prescriptive approach via an enforceable code that requires organisations to put in place particular governance, risk management or cyber security systems and controls, given the pace of technological change and adaptation of organisations. The principles-based regulatory approach should be retained.

Our members also suggest Government consider and consult further on whether the Australian Privacy Principles is the most appropriate place to mandate minimum cyber security standards. In Governance Institute's submission to the relevant Department of Home Affairs on this issue, we recommended that any cyber security governance standards be voluntary not mandatory, to reduce regulatory compliance burden.

We also advocate that Government consider the potential for regulatory confusion if the OAIC, ASIC, APRA, the Department of Home Affairs, the Australian Signals Directorate and the Australian Cyber Security Centre were to operate simultaneously in the area of cyber security regulation, standards setting and awareness raising. We believe there is a need for consolidation, not expansion, in this critical policy area.

Governance Institute recommends that Government consider and consult further on whether the Australian Privacy Principles is the most appropriate place to mandate minimum cyber security standards, given the need for consolidation, not expansion in this critical policy area.

Changes to Notifiable Data Breaches (NDB) scheme

Governance Institute broadly supports the current NBD scheme. Our members believe that timely disclosure is important to drive best practice. However, we support calls for greater clarity and more regulatory guidance, on the application of the NDB scheme, including practical examples of how to apply the threshold of 'serious harm'. Governance Institute members are aware of organisations facing practical challenges when attempting to interpret these provisions and

[9] Discussion Paper, page 146
[10] Discussion Paper, page 147

understand their compliance obligations. We also encourage Government to consider how it may increase the practical use of mandatory reports in threat intelligence gathering and awareness raising across industry. Breach reports should not just be a tick-box compliance exercise. They should be used to inform and assist industry and encourage best practice.

Governance Institute supports proposal 27.1 requiring organisations making breach notifications to include information on steps taken by way of remediation. We anticipate this will encourage organisations to strengthen their governance and risk management in relation to data and cyber security. This should be supported by regulatory guidance on best practice in these areas. However, the Government should consider the potential for this to reduce the timeliness of breach notifications.

It is important to note that some elements of the Discussion Paper may have the opposite intended effect of disincentivising reporting under the NDB scheme, especially the proposals for a direct right of action and a tort of privacy. Where potential losses from civil claims are significant, organisations may avoid voluntary reporting and may even be incentivised not to comply with their legal requirements. We encourage the Government to consider these potential unintended impacts.

We also note the proposal to introduce a new civil penalty provision that would enable the OAIC to take enforcement action for a single instance of failure to notify the OAIC or affected individuals of a data breach in a timely manner. This would differ from the current approach in Privacy Act section 13G that only empowers the OAIC to apply to the court for a civil penalty order where an entity's failure to notify constitutes a 'serious' or 'repeated' interference with privacy. Our members support the current approach where the OAIC may apply to Court where an entity's failure to notify constitutes a serious or repeated inference with privacy.

Governance Institute recommends that Government consider the potential unintended impacts of the introduction of direct action and tort of privacy. **We also recommend** Government reconsider the new civil penalty provisions that would enable the OAIC to take enforcement action for a single instance of failure to notify the OAIC or affected individuals of a data breach in a timely manner. Our members support the current approach in the Privacy Act.

Exemption for small business and NFPs

Privacy law is a highly specialised area that is challenging for smaller businesses and not-for-profits to navigate and comply with.

As noted in the Discussion Paper, the Privacy Act currently does not apply to businesses with an annual turnover of less than $3 million, which is estimated to exempt approximately 5 per cent of Australian businesses from the Act's scope and application.[11] What the Discussion Paper does not mention is that this exemption also applies to many not-for-profits, which are often even less capable than their commercial counterparts to comply with onerous levels of regulation. We note that one of the objects of the Australian charities regulator, the Australian Charities and Not-for-profits Commission's (ACNC), statutory objects is promoting the reduction of unnecessary regulatory burden on the sector. The ACNC actively promotes activities directed at achieving this object. Governance Institute is also a founding member of the #FixFundraising advocacy campaign that is urging a reduction in regulatory complexity in the area of charitable fundraising law. Our members are pleased to note that the Commonwealth Government is working with the states and territories on reform in this area. At the same time as regulations are improved in one area, we would not want to see smaller charities and not-for-profits subjected to unnecessarily onerous levels of regulation in another area.

We agree that the small business and not-for-profit sectors need to play a part in economy-wide efforts to promote Australia's cyber security posture and prevent privacy breaches. However, we believe this is best achieved through government support and awareness raising, rather than by removing the current exemption. For example, we understand that small businesses and NFP's represent a large proportion of the data flow volume at a global scale. There is an opportunity for

[11] Discussion Paper, page 40

the Australian Cyber Security Centre, which already has some resources, to do more in this space for small businesses.

We acknowledge, as noted in the Discussion Paper, that Australia's exemption for small organisations is not replicated in other comparable jurisdictions and that some have argued keeping the exemption in place may be a barrier to a GDPR adequacy decision.[12] These are valid concerns that warrant further investigation. However, our current view is that removing the exemption may impose an onerous and uneven compliance burden on the smaller organisations that choose to comply although not required to, and may be likely to result in high rates of non-compliance, adding the risk of significant breach penalties. This is supported by evidence from the European Union. In 2019, one year after the regulatory scheme took effect, the EU conducted a survey of 716 small business leaders in Spain, France, Ireland and the UK, which was at that time an EU member, that found 'widespread ignorance about data security tools and loose adherence to the law's key privacy provisions'.[13] It is our understanding that Australia's larger organisations already find it difficult to know when exactly to comply with the NDB scheme, as an example. This illustrates the challenge Australia's smallest organisations would face. We believe a non-mandatory regulatory approach focussed on the provision of free tools, educational resources and direct financial subsidies, rather than legal enforcement, has a higher chance of changing the behaviour of smaller organisations and successfully achieving the policy objective.

Our members note with approval the funding committed by the Government for a Digital Directors Training package in the 2019-20 Federal Budget, the expansion and enhancement of the Australian Small Business Advisory Services program as part of the Digital Economy Strategy 2030 in the 2021-22 Federal Budget, and the Government's announcement on 15 November 2021 of a Digital Ready Assessment Tool to help Australian businesses assess their digital maturity and digitise operations. We encourage the Government to continue to develop direct support and awareness raising measures for privacy protection and digital capability building in smaller organisations and not-for-profits, as an alternative to an increased regulatory compliance burden by removing the current exemption. There may also be opportunities for larger organisations to assist and encourage smaller organisations to enhance their privacy practices and cyber security posture.

Governance Institute recommends that the Government consult further on any proposal to remove or lower the $3 million annual turnover exemption, including with the not-for-profit sector.

Enforcement powers, mechanisms and penalties

Both the Discussion Paper and the exposure draft legislation propose enhanced enforcement powers for the OAIC and significantly increased penalties for breaches of the Privacy Act.

In principle our members support these measures. On the whole, they consider Australian organisations are putting in place and continuing to enhance their governance and risk management frameworks to protect the data of their customers. Enhanced enforcement measures will help promote corporate cultures that manage and address the risks of data breach and privacy intrusion appropriately. It will be important to apply a risk lens and a materiality qualification to these enhanced performance measures, so that there is a greater level of accountability imposed in the case of the more serious privacy breaches.

They do, however, note with caution the proposal to introduce a statutory levy to fund the OAIC's use of these expanded enforcement powers. Corporate Australia is subject to an increasing array of levies, including ASIC and APRA cost recovery. Given the potential for substantially increased compliance costs on Australian organisations from the Privacy Act's expansion, we encourage that this be considered further and that there be broader consultation on this proposal.

Governance Institute members in principle, support supports the proposed enhanced enforcement powers for the OAIC and significantly increased penalties for breaches of the Privacy

[12] Discussion Paper, pages 43-44

[13] European Union, 2019, 'Millions of small businesses aren't GDPR compliant, our survey finds', https://gdpr.eu/2019-small-business-survey/

Act. However they encourage further consideration of the statutory levy to fund the OAIC's use of these powers given the potential for substantially increased compliance costs.

Increased protections – right to withdraw consent, request erasure, and a direct right of action

Governance Institute supports in principle the introduction of these additional protective mechanisms. It is important that individual Australians, are able to enforce their privacy rights.

However, these rights, especially the right to erasure, should not be absolute. There should be exemptions, as there are under the GDPR, to allow for data to be retained for legitimate commercial and public interest purposes and to allow for compliance with other legislative regimes that require retention of information in certain circumstances that are set out in these regimes. Good governance of an organisation may require the retention of certain kinds of data, including to comply with regulation, inform the board and shareholders, for use in litigation, and to adequately respond to, and resolve, customer complaints. The introduction of a right to erasure is likely to require a phased approach, as the software used by Australian organisations may not immediately allow for deletion capability. It should also be noted that erasure is likely to be highly challenging for particular sectors to implement.

A direct right of action will also need to be carefully balanced to prevent abuses of process, an unnecessary high case load on the court system, and a deterrent to doing business in Australia.

Governance Institute defers to legal experts as to whether it is appropriate to introduce a statutory tort of privacy. However, in relation to these reforms, the Governance Institute considers that the current defamation regime and privacy laws in Australia are adequate, and if introduced, careful consideration must be given to the impact of this new tort on free speech, particularly in relation to the current exemptions in place for journalists. A robust direct cause of action mitigates against the need for a statutory tort.

Governance Institute in principle supports the introduction of these additional protective mechanisms but considers the right of erasure should not be absolute and there should be exemptions, as there are under the GDPR, to allow for data to be retained for legitimate commercial and public interest purposes and to allow for compliance with other legislative regimes.

Overseas data flows

Governance Institute welcomes the Government's consideration of overseas data flows. Many organisations now use cloud services that result in the transfer and/or storage of data to overseas jurisdictions. It is not always possible for organisations to specify data storage locations or contractually bind suppliers to comply with the APPs. Consequently, it can be challenging for organisations to comply with APP 8. Adopting a more straightforward process that allows for the transfer of personal information and storage across borders would be more in line with how data actually flows in a digitally based, global economy.

To further facilitate the free flow of information across borders, Governance Institute supports in principle the introduction of a mechanism to prescribe countries and certification schemes that are substantially similar to the APPs. This would provide much needed clarity in respect of the overseas privacy and data protection laws that would satisfy APP 8.2(a) requirements. It can be challenging for organisations to make such an assessment without obtaining specialist legal advice.

These businesses are a huge proportion of the data flow volume at a global scale. There is an opportunity for the Cyber Security Centre to do more in this space for small businesses; given it already has some resources. Consideration could also be given to the introduction of a 'safe harbour' or similar concept to facilitate the transfer of personal information across borders to overseas jurisdictions with broadly equivalent privacy and data protection laws to Australian privacy laws. Articulating minimum standards that organisations must comply with to disclose personal information to an overseas recipient would also encourage better privacy practices generally.

Governance Institute supports in principle the introduction of a mechanism to prescribe countries and certification schemes that are substantially similar to the APPs. **Governance Institute encourages** consideration of a 'safe harbour' or similar concept to facilitate the transfer of personal information across borders to overseas jurisdictions with broadly equivalent privacy and data protection laws to Australian privacy laws.

Greater coordination and harmonisation between legislative schemes and frameworks

There are a number of overlapping federal, state and territory regulatory frameworks that seek to protect the sensitive personal information of Australians as well as those that regulate, as noted above, the related area of cyber security. These include the Consumer Data Right, the amendments to the Security of Critical Infrastructure (SOCI) Act passed by Parliament in November 2021, the state and territory privacy legislation, the state and territory health records legislation, and the Government's new proposed ransomware notification scheme.

Put simply, there is a growing need to harmonise the various schemes, especially the interaction between the Australian Privacy Principles and the state-based health records legislation.

It is important to note that mandatory notification and reporting schemes appear to have become a preferred regulatory tool for addressing a range of policy issues. The NDB scheme, modern slavery reporting, mandatory cyber incident reporting under Part 2B of the SOCI Act, and potential ransomware reporting are some examples. We would urge Government to consider how these schemes interact. A scenario where organisations of all sizes are required to notify and report on an ever-widening array of issues may result in boards and management being distracted and taking a tick-box approach to compliance, rather than being proactive in addressing underlying issues, building capability, enhancing security awareness and seizing opportunities to innovate.

Governance Institute urges Government to consider how the various legislative schemes and frameworks interact, given the ever widening array of issues facing boards and management which may encourage a tick-box approach to compliance, rather than being proactive in addressing underlying issues, building capability, enhancing security awareness and seizing opportunities to innovate.

If you wish to discuss any of the issues raised in this letter, please contact me or Catherine Maxwell.

Yours faithfully,

Megan Motto
CEO