

Summary of Suggestions for Cyber Security Improvement

2023-2030 Australian Cyber Security Strategy Discussion

Dear Sir/Madam,

I would suggest considering these in review and update of the Cyber Security and Data Privacy legislation:

1. The organisations which collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall use an appropriate encryption method(s) to encrypt individual data securely in the data base of the organisation like the Credit card encryption method which has been used to reduce the likelihood of credit or debit card information being stolen. It makes it impossible to access the credit card information without the corresponding encryption key that lets the merchant and financial institution conduct their transactions. The software of the organisation shall de-encrypt the personal data of the individuals when needed.
2. The ACSC (Australian Cyber Security Centre) with ASIC (Australian Security and Investment Commission) and/or another identified government organisation shall conduct a yearly audit on the implementation of the Cyber Security and Privacy Act and other relevant guidelines to ensure the organisations are collecting, saving, handling, using, distributing, and processing personal data in accordance with the legislation.
3. The ACSC shall measure and identify the security rating of the organisations based on the level compliance with the Cyber Security and Data Privacy Act, this rating shall be available to public. The individuals shall understand the risk if they decide to share their sensitive personal information with a poorly data security rated organisation.
4. The organisations which cannot obtain adequate rating for compliance with the Cyber Security and Data Privacy Act cannot collect new sensitive personal information from individuals.
5. The organisations which cannot obtain adequate rating for compliance with the Cyber Security and Data Privacy Act shall destroy the sensitive personal information of current clients or appropriately make the already collected sensitive personal information data contained and unavailable to any potential cyber-attack.
6. The organisations which collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall erase previous clients after 3 years.
7. The organisations which need to collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall ask the customers the personal information which are very necessary for implementation of the application. Unnecessary information for marketing or other purposes rather than the main reason the individual is sharing their personal information shall not collected in the same process of application unless the individuals agree to share additional personal data.
8. The organisations which need to collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall use qualified experts to check and review the efficiency and reliability of their cyber security and

Summary of Suggestions for Cyber Security Improvement

2023-2030 Australian Cyber Security Strategy Discussion

data management systems. This audit shall be available and sent to the ACSC (Australian Cyber Security Centre) every year.

9. The organisations which need to collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall review their data base yearly to remove unnecessary record of data of individuals.
10. The organisations which need to collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall not share the individual data with other organisations which are not assessed and qualified by ASCS as a Secure Organisation.
11. The organisations which need to collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall conduct a cyber drill to ensure their systems and network is not vulnerable with a potential cyber-attack.
12. The organisations which need to collect, save, process, share, use, handle, and distribute the sensitive personal information of the clients or any individuals and businesses shall inform the individuals/clients the exact name of the organisations which the individual's sensitive data would be shared with clearly and ask for a permission, otherwise the organisation cannot share the sensitive personal information with other organisations.

I would like to receive feedback on this submission, it will be much appreciated.

Best Regards,
Nick Mahani

Email: [REDACTED]