Senate Economics References Committee's inquiry into the Influence of international digital platforms

ANSWERS TO QUESTIONS ON NOTICE
Digital Transformation Agency
22 August 2023

Department/Agency: Digital Transformation Agency
Type of question: Hansard, Page 14
Topic: Notifiable attack contact clauses
Date set by the committee for the return of answer: Tuesday, 5 September 2023
Question on Notice Number: DTA002

Number of pages: 2

Question:
Senator SHOEBRIDGE: What is a 'notifiable' attack?
Mr Fechner: It will be within the contract clauses. We can include that in our response to your question on notice.
Senator SHOEBRIDGE: Are you saying the contract clauses mirror perfectly the reporting obligations that are being put in place under the amended SOCI?
Mr Fechner: Our agreement with Home Affairs is that cloud providers that are certified strategic meet the threshold of the SOCI requirements.
Senator SHOEBRIDGE: One of the key things under the SOCI amendment was to have a regime in place so the Commonwealth could respond to a serious cybersecurity incident. They were meant to be coming up with new innovative, safety focused responses if there'd been a serious breach. Is that in place for these cloud services?
Mr Fechner: Again, we have significant contract clauses under all of the header agreements that require providers to notify us of these breaches. Our role would be not to work on the incident resolution but rather to make sure that it is referred to the appropriate functions in Home Affairs

Answer:

Under the Notifiable Data Breaches scheme any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved (*refer Part IIIC – Notification of eligible data breaches of the Privacy Act 1988*)

The Digital Transformation Agency (DTA) panels and arrangements follow the Australian Privacy Principles and the Privacy Act 1988. These provide requirements around data breach disclosures, including timelines and information around what is considered a notifiable breach. Any entity covered by the Privacy Act is also covered by the Notifiable Data Breach scheme, its definition, and the reporting requirements. The relevant clauses in our arrangements and panels refer to the Privacy Act 1988 for this reason.

The Cloud Marketplace panel provides clauses written into its head agreement regarding storing of data, reporting of privacy and its usage. These clauses are listed below for reference:

- 32. Privacy
- 32.2 seller must:
    - 32.2.1 comply with all privacy laws in respect of its collection, use, storage, or disclosure of personal information;
    - 32.2.3 carry out and discharge the obligations contained in the Australian privacy principles as if it were DTA under the Privacy Act;
- 32.3 Unless otherwise prohibited by law, seller must promptly notify DTA representative (in respect of this head agreement) if seller:
    - 32.3.1 becomes aware of an actual breach or suspected breach of any of its privacy obligations;
    - 32.3.2 becomes aware that a disclosure of personal information is required by any applicable laws;
- 4.8.3 if buyer seeks to store data (other than publicly available data) in the cloud, for each cloud service, seller must, if specified in the cloud marketplace contract, undertake the following:
    - Gateway certification by the Australian Signals Directorate (ASD) (https://www.cyber.gov.au/irap/asd-certified-gateways);
    - IT security audit by a certified Information Security Registered Assessors Program (IRAP) assessor (or equivalent assessment);
    - security vetting of seller personnel in accordance with the Australian Government Security Vetting Agency (AGSVA);
    - comply with 'Strategies to Mitigate Targeted Cyber Intrusions' by ASD; and
    - comply with requirements stemming from other relevant Australian Government strategies and policies that may impact data security at present and in the future.

- The Amazon web service (AWS) whole-of-government agreement provides instruction regarding notifiable data breaches including security and privacy information.
    - Clause 3. Privacy and Security, provides an overview of the requirements, and also references the AWS Australian Notifiable Data Breach Addendum which provides detailed information and instruction.

- The Microsoft Business and Services Agreement also contains clauses to cover any data breach concerns under Clause 16. Privacy and compliance with laws.
- Additionally, clause 16.d. provides specific information related to data breach notifications.
    - Microsoft will notify Customer of any Security Incident in accordance with, and will comply with its other obligations under, the Security Incident Notification section of the Online Services Terms.

On receipt of such notice Customer must take reasonable steps to carry out, within 30 days, an assessment to determine whether there are reasonable grounds to believe that an Eligible Data Breach (as defined in the Privacy Act) has occurred.