From: [redacted]
To: FeedbackRTIandprivacy
Subject: Privacy Legislation Feedback
Date: Friday, 3 February 2017 4:33:10 PM

Dear Team,

I am writing in response to the consultation for the review of privacy legislation. My feedback concerns Question 27. Please note the following is my opinion and does not represent the Department's position.

27. Does section 33 create concerns for agencies seeking to transfer personal information, particularly through their use of technology? Are the exceptions in section 33 adequate? Should section 33 refer to the disclosure, rather than the transfer, of information outside Australia?

I work in the ICT Procurement field with a legal background. The Government's policy to consider as-a-service (or cloud computing) first has required my team to work through cloud computing as a preference. I understand this policy intends to reduce spend on dated ICT hardware and infrastructure. It further encourages small companies to establish innovative solutions for government in a timely and cost effective way. Further, customers, including government are pushing suppliers to have apps and online portals for 24/7 self-service. This means suppliers other than traditional ICT suppliers are moving into cloud computing e.g. buying stationary online now includes an online portal.

Section 33 makes using technology more difficult as many services are hosted overseas. Some are hosted in several countries for the purpose of business continuity.

I have regularly encountered several issues with section 33 that should either be removed, or guidance material received to remove confusion.

1. Suppliers often argue that the storage of personal information overseas does not amount to a transfer. This has not been defined in a manner that would allow government agencies to rely on with minimal risk. As such, agencies have taken very broad interpretations of the word transfer out of fear. If transfer was changed to disclosed, this would also have to be defined. What if the data is stored in Australia, but the support team is overseas and can access the data from outside of Australia, yet the location of the data did not leave Australia, how would this comply?
2. Authority to approve the disclosure of personal information outside of Australia is also unclear. The information security classification framework requires agencies to classify the data and identify a data owner. Some believe this data owner (often a mid-level manager/director) has the authority to approve the personal information be dealt with in any manner. However others don't consider this to be sufficient authority, especially given the consequence of a breach. The legislation has not given the authority to the Minister or DG, as such, many agencies have not drafted delegation documents as there is no authority to delegate. Yet the political and reputational risks, not to mention the risks to the individuals, would suggest the authority should be granted to someone with an understanding of the risks. Perhaps the CIOs of each entity, rather than all executive directors. The actual instruments of delegation would be an agency to agency concern, however I would have thought commentary by the OIC would be beneficial here.
3. There is no distinction between how the data is gathered.
    a. Public citizen's data collected by the government should of course receive the upmost care and attention. It is reasonable to pay $10,000 per annum for penetration test and conduct other due diligence to ensure the data is stored securely. The assessment of bulk datasets is reasonable.
    b. Staff data however is interesting. Is the agency required to ask all external parties

with where their email servers are located prior to a staff member emailing the external party. Staff are required as part of their job to email external parties on a regular basis. If the external party uses and overseas hosted email server, then the staff member's name, work email and work phone details are transferred overseas. There is no guidance on whether staff have to be aware of the location of where their data is being transferred to before consent is valid. Further, is it reasonable that agencies are required to interrogate all email server locations?

4. The effect section 33 has, is that if the data is stored in Australia, there is little concerns for the security of the data. The information security framework still requires a minimum standard of security, however this does not appear to have any teeth compared to section 33. As such, I have experienced occasions where local storage in someone's unsecured shed in a flood prone area is easier to receive approvals for than it is to receive approvals for an international reputable company to host the data.
5. The meaning of reasonable efforts is also unclear. In the past I have requested advice on what steps are considered reasonable efforts. In my opinion, compliance with the Information Security Classification Framework would be considered reasonable steps. However, I have worked with managers who not only want the core hosting system to meet this standard, but also the billing system and the vendor's email servers. It should be noted those systems are only likely to contain the finance and contract manager's contact details. The risk with expanding assessments beyond the core system include limiting the supply chain to very small local vendors who could otherwise be considered high risk.
6. Regardless of any changes, I believe DGs should receive specific training in this area. Most agencies required the DG to approve data leaving Australia. DG's should be armed with information to ensure they understand the risks and the legislation. There have been a few occasions in my experience across agencies where DGs have refrained from giving approval where the legislation does allow the transfer. The reluctance to approve demonstrates a level of discomfort with the legislation that could be addressed by targeted training to the approver.

Regards,

Samantha Rose (Lowry)
Procurement and Contracts Manager
Information Services Directorate | Department of Housing and Public Works
Level 15 | 41 George Street | Brisbane
[redacted] | www.hpw.qld.gov.au |
www.qld.gov.au/housing

Customers first | Ideas into action | Unleash potential | Be courageous | Empower people | Healthy and safe workforce

nature) for detection of viruses, malicious code, SPAM, executable programs or content it deems unacceptable. All reasonable precautions will be taken to respect the privacy of individuals in accordance with the Information Privacy Act 2009 (Qld). Personal information will only be used for official purposes, e.g. monitoring Departmental Personnel's compliance with Departmental Policies. Personal information will not be divulged or disclosed to others, unless authorised or required by Departmental Policy and/or law.

Thank you.