Feedback on PDPA consultation paper

Name of person: Richard Neo

In the capacity of an individual and consumer

Questions:

Q1. What are your views on the impact of data portability, specifically on consumers, market and economy?

Ans 1) The impact could be positive and negative. When it comes to positive impact, consumers could access readily available personal data to apply for things like mobile data plans and switch between service providers. This could enhance efficiency of transactions and payments, thereby speeding up the velocity of money flows and increase national income. The market will become more dynamic with more intense competition which could reduce prices for consumers. However, with high speed of data portability, data security could be potentially compromised as a trade-off against the convenience and efficiency attained as organisations may do away with necessary security measures which could impede the speed of porting personal data from one organisation to another.

Q2. What are your views on the proposed Data Portability Obligation, specifically –
a) scope of organisations covered; and
b) scope of data covered?

Ans 2) a) As regards the scope of organisations covered, I am more concerned about the those organisations in the private sector that a public agency or any government-linked organisation outsource data processing and installation & maintenance of security systems (involving personal data too) to. If such organisations are exempted from Data Portability Obligation and the contractor in the private sector who obtain such contract to manage the Data Portability job without any Data protection capabilities or Data Protection Trust Mark, then we could see more cases of data leaks and successful hacking incidents like Singhealth cyberattacks and the data of NSmen being leaked by computer vendor Option Gift (June 2018)

So with exemption from the Portability Obligation under the PDPA, will it mean they will not be held responsible for any data leak due to lack of robust cybersecurity protection?

My suggestion is for the government-linked organisations or public agency to only outsource its contracts to vendors who have attained the DPTM (Data Protection Trade Mark) and those private firms without such certification will be denied access to any public project. This could help increase awareness of the importance of DPTM certifications and encourage more firms to strive hard to attain such certifications in order to have access to public projects and contracts.

I myself have observed some private firms take very little notice of the importance of cybersecurity and data protection. If the public projects or contracts are outsourced to such firms, the data of the public will be at higher risk of being leaked, stolen and abused.

Q6. What are your views on the proposed binding codes of practices that set out specific requirements and standards for the porting of data in specific clusters or sectors?

Ans 6) I am more concerned with part (d) " **Security of data**: minimum standards to ensure the protection of data during transmission and the integrity and security of participating systems." Is the minimum standards sufficient to ensure protection of personal data during transmission and the integrity and security of participating systems. How is the "minimum standards" defined? If there is lapse in the organisations handling personal data that led to a data leak like the Singhealth hacking incident and RedCross data leak, will there be any financial liability and penalties that the organisations are ready to pay? If the data is transmitted via wireless mode, the risks of being hacked is even higher. So how will the organisations going to ensure such risks will be minimised?

My suggestion is to make it mandatory for firms which secured contracts to manage, handle data portability requests or selling devices/software for such purposes with data storage functions to attain DTPM status and have devices/software certified to be safe by experts. If not, they cannot qualify for bidding for contracts from government bodies or government-linked organisations. This could encourage firms to have trained staff to ensure safety of data being ported and increase awareness of the importance of data security with more firms attaining DTPM status.

Conclusion: I believe the public will be more concerned with data protection more than data portability. So in setting the necessary standards for the porting of data un specific clusters or sectors, it is best to have sufficient measures to ensure parties in charge of porting of data have the sufficient cybersecurity capabilities so that the minds of public can be at ease. I strongly believe too that many members of the public do not wish to let their personal data fall into foreign hackers or crooks and expose their finances to greater risk of losses. Portability of data may bring great benefits but certainly not at the expense of the data security of cosumers.