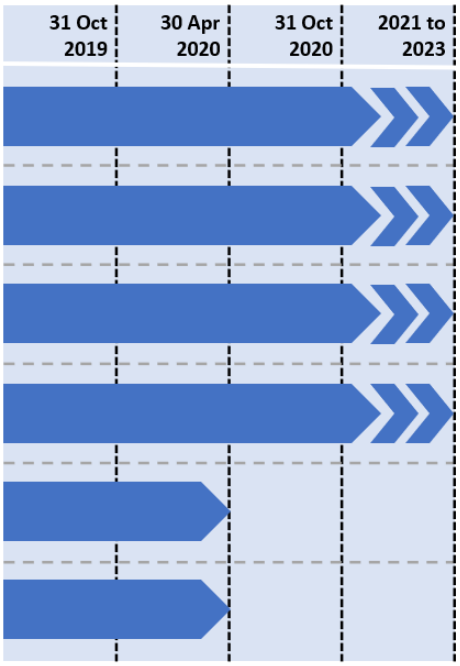
Annex

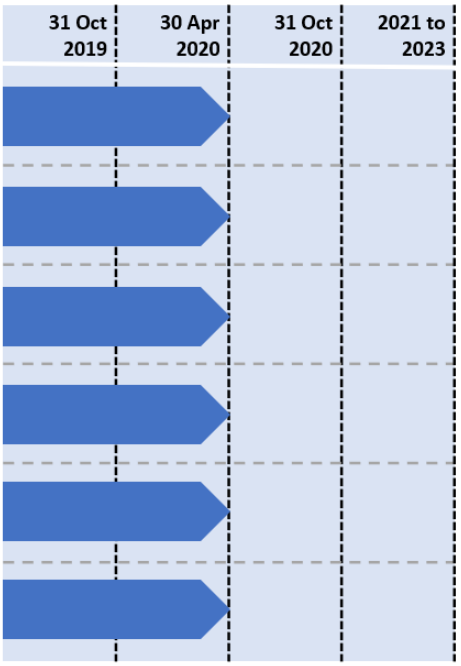
Implementation Timeline of the Public Sector Data Security Review Committee Recommendations

(Extracted from Annex J of the Public Sector Data Security Review Committee Report published on 27 November 2019)

Key Recommendation 1	
1.1	Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads
1.2	Enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity
1.3	Protect the data directly when it is stored and distributed to render the data unusable even if extracted
1.4	Keep abreast of advanced technical measures and deploy them when they are mature
1.5	Enhance the data security audit framework to detect gaps in practices and policies before they manifest into incidents
1.6	Enhance the third party management framework to ensure that third parties handle Government data with the appropriate protection

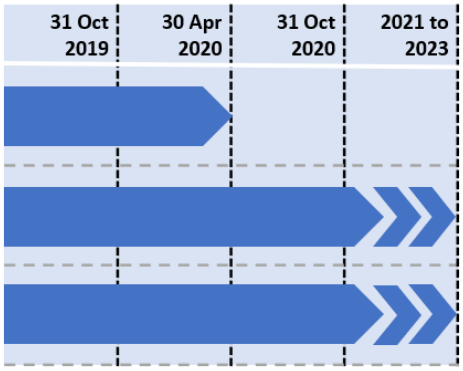


Key Recommendation 2	
2.1	Establish a central contact point in the Government Data Office for the public to report Government data incidents
2.2	Designate the Government Data Office to monitor and analyse data incidents that pose significant harm to individuals
2.3	Designate the Government IT Incident Management Committee to respond to incidents with Severe impact
2.4	Institute a framework for all public agencies to promptly notify individuals affected by data incidents with significant impact
2.5	Establish a standard process for post-incident inquiry for all data incidents.
2.6	Distil and share learning points with all agencies to improve their data protection policies/measures and response to incidents

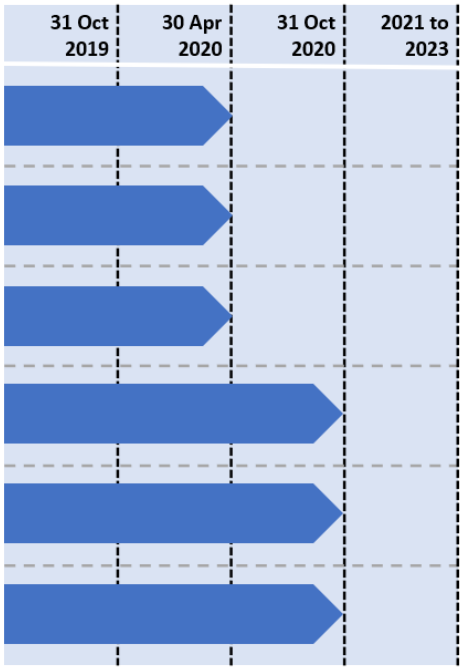


Smart Nation SINGAPORE

Key Recommendation 3	
3.1	Clarify and specify the roles and responsibilities of groups of public officers involved in the management of data security
3.2	Equip these groups with the requisite competencies and capabilities to perform their roles effectively
3.3	Inculcate a culture of excellence around sharing and using data securely



Key Recommendation 4	
4.1	Institute organisational Key Performance Indicators (KPIs) for data security
4.2	Mandate that the top leadership be accountable for putting in place a strong organisational data security regime.
4.3	Make the impact and consequences of data security breaches salient to public officers
4.4	Ensure accountability of third parties handling Government data by amending the PDPA
4.5	Publish the Government's policies and standards on personal data protection
4.6	Publish an annual update on the Government's personal data protection efforts



Key Recommendation 5	
5.1	Appoint the Digital Government Executive Committee to oversee public sector data security
5.2	Set up a Government Data Security Unit to drive data security efforts across the Government
5.3	Deepen the Government's expertise in data privacy protection technologies through GovTech's Capability Centres.