SMART NATION & DIGITAL GOVERNMENT OFFICE

SECOND UPDATE ON THE GOVERNMENT'S PERSONAL DATA PROTECTION EFFORTS

2021

Introduction

1. In March 2019, PM Lee convened the Public Sector Data Security Review Committee (PSDSRC) to review how the Government is securing and protecting citizens' data from end-to-end, and to recommend measures and an action plan to improve the Government's protection of citizens' data and response to incidents. One of the PSDSRC's recommendations was for the Government to publish annual updates on its data security efforts to provide the public with greater visibility over its approach to data security and data protection.

2. This publication is the second update on the Government's efforts to safeguard personal data ("Update"). It outlines what the Government has done in the past financial year (FY 2020) to strengthen the public sector data security regime.

Background

3. The number of data breaches globally has been growing in recent years, and this trend has accelerated in the past year. The total number of records exposed in 2020 was reported to be around twice that of 2019[1]. In Singapore, the number of complaints made to the Personal Data Protection Commission (PDPC) on potential personal data breaches by private organisations has also been on the rise[2].

4. This could be due, in part, to the COVID-19 crisis accelerating the pace of digitalisation in the past year, as many businesses are forced to conduct their activities online in light of public health restrictions. As more transactions occur digitally and more data is generated and exchanged, this increases the risk of data being exposed or exfiltrated. Work-from-home arrangements and the use of unsecured home networks may also raise the risk of data incidents.

5. These trends highlight the increased data security risks faced by the private and public sectors and the importance and urgency of implementing the necessary measures to safeguard personal data.

---

1 Source: RiskBased Security 2020 Year End Report

2 No. of complaints made to PDPC from 2018 to 2020 were as follows:
- Year 2018: 2,700
- Year 2019: 4,500
- Year 2020: 6,100

Trends in Number of Government Data Incidents Reported

6. 108 data incidents were reported in FY2020, up from 75 in FY2019. This was a 44% increase in the total number of data incidents reported. The data incidents reported in the period from FY2018 to FY2020, broken down by the Government's incident severity classification[3], is as follows:

Total Number of Data Incidents Reported (by Severity)			
Data Incident Severity	**FY2018**	**FY2019**	**FY2020**
Low	10 (19%)	33 (44%)	64 (59%)
Medium	35 (69%)	37 (49%)	44 (41%)
High	4 (8%)	5 (7%)	0 (0%)
Severe	2 (4%)[4]	0 (0%)	0 (0%)
Very Severe	0 (0%)	0 (0%)	0 (0%)
Total	**51**	**75**	**108**

Table 1

[3] The severity of a data incident is assessed based on the impact on the national security or national interests, as well as the impact on the individual or entity. Details of the incident severity classification framework can be found in Annex B.

[4] The two "Severe" incidents in FY2018 were 1) the unauthorised disclosure of the records from MOH's HIV registry reported in the public domain in January 2019 and 2) the discovery of a vulnerability in the State Court filling system as reported in the public domain in November 2018.

7. The marked increase in data incidents reported correlates with trends seen in the private sector and globally, as the exchange and usage of data grows. The increase is also due, in part, to an improved understanding amongst officers to report all data incidents, no matter how small. Even though there was a rise in the number of data incidents in FY2020, all of the incidents were assessed to be of "Low" or "Medium" severity. None of the FY2020 incidents were assessed to be of "High" severity or worse. From FY2018 to FY2020, there has been a general downward trend in the number of data incidents assessed to have severity of "High", "Severe" or "Very Severe".

8. In FY2020, we addressed all data incidents within 48h hours of detecting the incident, despite the increase in the number of data incidents.

Total Number of Data Incidents Reported (by Time Taken to Address)			
Time taken to address data incident	**FY2018**	**FY2019**	**FY2020**
Within 48h of detection	50	75	108
Between 48h and 7 days	1	0	0
Total	**51**	**75**	**108**

Table 2

Overview of Progress in Enhancing the Public Sector Data Security Regime

9. To enhance the public sector data security regime, the PSDSRC made five key recommendations to achieve five desired outcomes (Table 3). The Government accepted the PSDSRC's recommendations in full and committed to implement them in phases from 2020 to end-2023.

Desired Outcomes	Key Recommendations
Protect data and **prevent data compromises**	1. Enhance technology and processes to effectively protect data against security threats and prevent data compromises.
Detect and respond to data incidents	2. Strengthen processes to detect and respond to data incidents swiftly and effectively.
Competent public officers embodying a **culture of excellence**	3. Improve culture of excellence around sharing and using data securely and raise public officers' competencies in safeguarding data.
Accountability for data protection at every level	4. Enhance frameworks and processes to improve the accountability and transparency of the public sector data security regime.
Sustainable and resilient data security regime	5. Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime that can meet future needs.

Table 3

Progress of implementing the PSDSRC's Recommendations

10. As of 31 March 2021, 21 of the 24 initiatives formulated to operationalise the five key recommendations have been implemented[5] as planned (see Annex A for the full list of recommendations). Since the inaugural Update was published in November 2020, 3 more initiatives have been implemented:

    a. The Data Privacy Protection Capability Centre (DPPCC) was established in GovTech in December 2020 to deepen the Government's expertise of data privacy protection technologies (Recommendation 5.3).

    b. Since its inception, the DPPCC has also begun studying and implementing advanced technical measures to protect data in Government systems, such as de-identification modules to protect sensitive personal data (Recommendation 1.4).

    c. Amendments to the Personal Data Protection Act (PDPA) came into force on 1 February 2021; these amendments strengthen the accountability measures on non-Government entities and non-Public Officers who handle Government data (Recommendation 4.4).

    The remaining 3 initiatives are technical measures (Recommendation 1.1 to 1.3) which require significant re-architecting of technical systems and therefore take more time to develop. These initiatives had been envisaged to be completed by end-2023. The Government is on track to complete these initiatives as planned.

11. These efforts continue to strengthen the Government's capabilities to safeguard data, amidst an increasingly complex operating data security environment. With these initiatives in place, we have seen:

    a. Improved audit and third-party management processes;

    b. Enhanced data incident management processes;

    c. Strengthened data security accountability measures;

    d. A clearer and more structured approach to improving data security competencies and building a data security-conscious culture;

    e. Strengthened data security organisational structures;

    f. Improved transparency of the public sector data security regime; and

    g. Sustained efforts in implementing data protection capabilities.

---

5 As of 31 October 2020, 18 of the 24 recommended initiatives had been implemented. Between 31 October 2020 and 31 March 2021, 3 more initiatives had been implemented, as planned, for a total of 21 initiatives implemented.

Highlights of Government's Initiatives to Strengthen Data Security from 1 October 2020 to 31 March 2021

12. The first Update published on 11 November 2020 covered the Government's initiatives from the date of publication of the PSDSRC Report on 26 November 2020 up to 30 September 2020. This present Update covers the Government's efforts to achieve the outcomes in Table 3, during the period from 1 October 2020 to 31 March 2021. Subsequent Updates will be published annually, covering the preceding financial year.

Outcome 1: Protect data and prevent data compromises

13. The Government has and will continue to implement a combination of technical and process measures to minimise the risk of data compromises[6] (Recommendations 1.1 to 1.3). In July 2020, the PSDSRC recommended technical and process measures were incorporated into the Government Instruction Manuals to give clear guidance to public agencies on the requirements and standards of the data security measures. An overview of these measures has also been made available to the public on the Smart Nation website.

---

6 In October 2019, the Government implemented the following measures:

a. An email data protection tool that requires officers to affirm that they intend to send an email with sensitive data to prevent any accidental or unauthorised disclosure through email.

b. A requirement for officers to password-protect files containing sensitive data when sending them out, and to securely distribute the passwords through a separate channel. This ensures that only the recipient with the password can access the file.

c. Tools to check the integrity of files containing sensitive data to ensure that they are not altered during distribution.

14. The technical and process measures have been effective in mitigating the impact of potential data compromises. For example, the process measure of protecting files with passwords and sending the passwords via a separate channel, prevented at least one data incident in FY2020 from escalating further. In one incident, an email with files containing sensitive personal data was mistakenly sent to employees of a government agency who were not authorised to receive the files. Fortunately, the files were password protected and the public officer who sent the erroneous email realised his mistake when preparing to send the password through a separate channel. Email recipients were unable to open the files without the password and no data was disclosed.

15. The Government has also been working on implementing the complex technical solutions recommended by the PSDSRC (Recommendation 1.2), to further strengthen the public sector's data security posture.

16. In November 2020, the Government launched the Government Commercial Cloud (GCC) Privileged Identity Management (PIM) solution. With more Government systems migrating to the Commercial Cloud as part of our "Cloud-First" strategy, the PIM solution ensures that access by privileged users (i.e. users who have wide access to a range of data), such as system administrators, will be secured and monitored to prevent unauthorised use. The GCC-PIM is a central solution that agencies can readily subscribe to, rather than develop bespoke PIM solutions for each of their systems in the GCC; this saves agencies time and effort in securing their systems.

17. The Government has also started to develop WOG Data Loss Protection (DLP) services. The DLP services use technical and process controls to detect anomalous activities, such as unexpected downloads of large amounts of data to personal computers, that are indicators of possible malicious activity or data incidents. When such activities are detected, the DLP services will prompt the user to take certain actions, such as confirming that the data was intended to be transferred before proceeding to do so. In some cases, the DLP services will stop the anomalous data transfer altogether to prevent any loss of data. The implementation of the WOG DLP services will commence by the end of 2021.

18. The Government has also continued to strengthen its management of third parties that handle Government data (Recommendation 1.6). These vendors may have access to large volumes of Government data, and it is vital that the Government's high standards of data protection are extended to these third parties. Templates with standard terms and conditions, as well as the necessary data security requirements, have been designed for agencies' use when calling for ICT tenders. Beyond this, multiple engagement sessions with agencies were held, to ensure that they have a good grasp of the new third party management framework and know how to manage their vendors well.

Outcome 2: Detect and respond swiftly to data incidents

19. While we implement technical and process measures to prevent data compromises, it is not possible to eliminate data incidents altogether. When a data incident occurs, we need to detect and respond to it swiftly.

20. The Government Data Security Contact Centre (GDSCC) was established on 30 April 2020 for members of the public to report data incidents involving government data or government agencies [7]. The GDSCC is intended to augment the Government's capabilities to detect data incidents, and through it, the Government works with data security professionals and members of the public to enhance the security of data.

21. In FY2020, the GDSCC received 119 reports, of which 6 were classified as "Data Incidents" upon further investigation:

No. of Data Incidents Reported through GDSCC	
Incidents Reported	**FY2020**
Incidents classified as "Data Incidents" upon further investigation	6
Incidents not classified as "Data Incidents"	113[8]
Total Incidents Reported to GDSCC	**119**

Table 4

7 Members of the public are encouraged to report Government data incidents to GDSCC via the online platform at https://smartnation.gov.sg/report-data-incident.

8 113 incidents reported to GDSCC were not related to government data. Examples of such reports include queries on advertisement/promotion calls and texts when members of the public had opted out of the Do Not Call registry and texts offering loans or gambling opportunities. These reports were subsequently referred to the appropriate departments to handle.

22. All incidents and queries were resolved in a timely manner, and in accordance with established service standards, as shown in Table 5 below.

Categories	Definitions	Required Response Time	No of queries
Simple	Simple cases refer to straightforward queries with information ready	Within 3 working days	95
Standard	Standard cases refer to cases which require some investigation by the affected agency	Within 10 working days	10
Complex	Complex cases refer to cases which require significant investigation, and may have cross-agency involvement	Within 15 working days	14
Total			**119**

Table 5

23. The GDSCC complements the Government's Vulnerability Disclosure Programme (VDP) that was launched in October 2019[9], for members of public to identify and report the discovery of vulnerabilities found in Government internet-facing web-based and mobile applications used by citizens, business and the public sector. Concurrently, the Government has been running a series of Bug Bounty Programmes (BBP) where members of the cybersecurity community help to discover vulnerabilities within a fixed set of systems over a limited period of time. As of March 2021, the VDP and BBP have received more than 1000 vulnerability reports, out of which 496 were assessed to be valid vulnerabilities.

24. The enhanced public sector Data Incident Management Framework was introduced in July 2020, to manage data incidents in a coordinated and effective manner across the public sector (Recommendation 2). The enhanced Framework has enabled the Government to address data incidents expeditiously; in FY2020, all data incidents reported were addressed within 48 hours of detection (see Table 3), despite an increase in the number of data incidents.

9 Source: https://www.tech.gov.sg/files/media/media-releases/2019/May/Annex - Factsheet on Vulnerability Disclosure Programme.pdf

25. Beyond what was recommended by the PSDSRC, the Government has also instituted a requirement for all public agencies to carry out cyber and data security incident exercises annually. These exercises simulate data incidents and test the readiness of agencies to effectively contain and manage the impact of the data incidents. To complement agency-specific exercises, the Government will also be conducting central ICT and Data Incident Management exercises involving multiple agencies to test the Government's ability to coordinate across agencies and provide a coherent WOG response. 4 ministries have been selected to participate in the inaugural central ICT and Data Incident Management Exercise to be held in September 2021.

Outcome 3: Competent public officers embodying a culture of excellence

26. The Government has continued to implement initiatives to ensure that public officers are well-equipped to protect data, and to instil in every public officer a culture of excellence in using data securely (Recommendation 3.3).

27. In February 2021, the Government refreshed the Data Security e-learning module[10] to include new content on how to work from home securely, and how to safeguard data when using the new Secure Internet Surfing technology[11] implemented in November 2020.

28. The Government has also started work on a series of engagement campaigns, targeted at all public officers, to be launched from May 2021. These campaigns are intended to raise officers' awareness of the importance and benefits of using data securely, as well as to provide practical steps that officers can take to use data securely in their daily work. Initiatives include regular newsletters to all public officers, virtual roadshows to drum up excitement about data security, a revamped intranet portal for officers to access information on how to use data securely, as well as toolkits and handbooks for reference.

29. In addition, the Government will be conducting a series of specialised workshops from July 2021 onwards for Key Appointment Holders and for ICT and data teams. Key Appointment Holders, such as Chief Data Officers and Chief Information Officers, play a critical role in driving and monitoring data security policies and measures, while ICT and data teams are directly responsible for implementing and managing the operations of data security measures within their respective systems and projects. These workshops and other specialised training opportunities will be crafted to equip them with the necessary skillsets to fulfil their roles.

30. Instilling a culture of excellence is a long-term endeavour and will require sustained efforts across many years at all levels of the organisation, especially for a large organisation like the Public Service. Human error is currently the largest source of government data incidents reported (see paragraph 34); we will continue to step up our efforts to develop our people's capabilities and instincts in managing and securing data.

---

10 All officers are required to complete, annually, the e-learning module on data security, including an accompanying quiz and a declaration that they have understood their responsibilities and liabilities in handling Government data. New hires are to complete the module within 3 months of joining the public agency. The annual e-learning programme was launched on 8 May 2020, as one of the recommendations by the PSDSRC.

11 Internet Surfing Separation was launched in 2016 and fully rolled out across the public service in 2017, in order to enhance the cybersecurity posture of the public sector. The Government implemented Secure Internet Surfing (SIS) for public officers from 2 November 2020. SIS is enabled by remote browsing technology and provides public officers with secure Internet access on their work laptops.

Outcome 4: Accountability for data protection at every level

31. The Government has enhanced the accountability frameworks and legislative measures to hold leaders, individuals and organisations accountable for protecting Government data.

32. *(New)* PSDSRC Recommendation 4.4 was implemented in November 2020, when amendments were introduced to the Personal Data Protection Act (PDPA) to hold third parties accountable for any mismanagement of government data. With the amendments, the PDPA will now:

    a. Cover all non-Government entities, including agents of Government. Previously, agents of Government (i.e. non-Government entities that were legally authorised to act on behalf of the Government) were not covered under the PDPA or the Public Sector (Governance) Act (PSGA). They were subject to the obligations in their contracts with public agencies and, where applicable, laws such as the Official Secrets Act. With the amendments to the PDPA, all non-Government entities will be covered under the PDPA, regardless of whether they are agents of the Government.

    b. Include accountability measures for non-Public Officers who recklessly or intentionally mishandle any personal data. This includes unauthorised disclosure of personal data, the misuse of data for a gain or to cause harm and the unauthorised re-identification of anonymised data. The new PDPA provisions mirror how the PSGA holds public officers accountable for egregious mishandling of Government data. With the PDPA amendments, non-Public Officers will be taken to task when data incidents occur, and these individuals will be held accountable for data lapses that are directly or indirectly caused by egregious mishandling of personal data.

The PDPA amendments came into force on 1 February 2021.

33. Beyond the PSDSRC recommendations, the Government has incorporated the need for high data protection standards and strong accountability for data in our response to the COVID-19 pandemic. In February 2021, the Government introduced the COVID-19 (Temporary Measures) Amendment Bill on a Certificate of Urgency to clearly specify the purposes for which personal contact tracing data collected by a digital contact tracing system can be used, and the accountability measures for the misuse of the data. (see Box 1). This was intended to give legal form to the statements made in Parliament that such data would only be used for investigation or proceedings in respect of serious offences, apart from contact tracing.

Box 1: Digital Contact Tracing Systems and Part 11 of the COVID-19 (Temporary Measures) Act

It is important that the Government makes full use of data and technology to support our fight against COVID-19. Digital tools such as TraceTogether and SafeEntry have enabled the Ministry of Health to shorten the average time required for contact tracing from 4 days to less than 1.5 days. Individuals who have been exposed, or potentially exposed, are isolated more swiftly, reducing the probability of them passing on the virus within the community.

The Government introduced the COVID-19 (Temporary Measures) (Amendment) Act in February 2021 to clearly spell out the purposes for which the Government can use such data, and the accountability measures for the misuse of the data. The legislation specifies that the Government can use personal contact tracing data (collected through digital contact tracing tools) only for contact tracing, except for investigations or criminal proceedings in respect of serious offences. These are offences of a significant severity and/or pose an immediate threat to life or public safety, such as use of firearms and dangerous weapons, terrorism, murder, drug offences that attract death penalty, kidnapping and rape.

Any unauthorised disclosure or use of the data will be a criminal offence; public officers found guilty of such an offence may be liable to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 2 years or to both. These penalties are higher than those provided in the PSGA for similar offences, to signal the gravity of undermining trust in our digital contact tracing systems during our fight against COVID-19.

The legislation to limit the use of personal contact tracing data was enacted in exceptional circumstances, during a time of pandemic. The legislative amendments were introduced on a Certificate of Urgency to provide the assurance that the data would be properly safeguarded and used only for the appropriate purposes, so that we could focus our attention on battling COVID-19.

Part 11 of the COVID-19 (Temporary Measures) Act came into force on 1 March 2021.

34. The Government will not hesitate to take action against individuals who use or disclose Government data without authorisation. A number of individuals involved in unauthorised disclosures of information relating to Singapore's response to COVID-19 have been charged under the Official Secrets Act (see Box 2.)

Box 2: Public officers charged for wrongly communication of COVID-19 related information.

A number of public officers had been charged under the Official Secrets Act (OSA) for disclosing official information without authorisation.

- In April 2021, 2 public officers were charged under the OSA. A former personal assistant to the Director-General of the Singapore Food Agency (SFA) was charged for leaking an unreleased statement about school closures during COVID-19 circuit breaker. A former Deputy Lead of the Ministry of Health was charged for leaking Singapore's daily COVID-19 case numbers on 22 occasions last year.

- In May 2021, a Deputy Director at the National Library Board was charged for leaking information on the resumption of activities in Phase Two of Singapore's reopening in Jun 2020.

- In May 2021, a 32-year-old public servant was arrested under the OSA for allegedly leaking information about COVID-19 measures for sports and physical activities to individuals in a private WhatsApp chat group who were not authorised to receive the information.

Outcome 5: Sustainable and resilient data security regime

35. (New) The frontier of data privacy protection technology is rapidly shifting, and the operating context for using data securely is becoming more complex. To keep up with emerging threats and new technologies, the Government established the Data Privacy Protection Capability Centre (DPPCC) on 31 December 2020, to deepen our capabilities and expertise in data privacy protection technologies (Recommendation 5.3). The DPPCC will also address PSDSRC Recommendation 1.4 by:

    a. Developing the Government's capabilities in data privacy protection technology solutions, including advanced data protection technology, both for WOG and for Agencies.

    b. Implementing these solutions to maintain data privacy while enabling data to be used.

    c. Providing consultancy services to agencies that face difficulty implementing data privacy protection technologies.

    d. Monitoring emerging data privacy protection risks and recommend solutions to mitigate these risks.

What's Next

Lessons from the Data Incidents and Data Security Initiatives

36. The Government's initiatives have helped to improve the public sector's data security posture, however, data incidents have continued to occur; this was primarily due to human error. With Work-from-Home arrangements and more discussions taking place via emails and digitally, there were more incidents of officers sending information to the wrong email address. There were also instances where public officers forgot to include external recipients in large mailing lists in the "bcc" instead of the "to" field to protect the privacy of recipients. Some officers forwarded information or documents to their private email accounts to ease the process of working from home on their personal devices. The officers found responsible for these data incidents had been counselled. Where required, officers have also been duly disciplined, with punitive measures ranging from formal reprimands to financial penalties.

37. The planned technical tools will help to prevent some of these incidents. For example, the WOG Data Loss Protection (DLP) services can flag out or stop anomalous activity for timely response.

38. We will also continue our efforts to inculcate data security consciousness in all public officers. The Government has embarked on several educational campaigns to increase data security awareness in the last year. This requires a sustained and continuous effort across many years.

39. Beyond that, we will continue to work with the cybersecurity and data security community, as well as the members of the public, through programmes such as the GDSCC, BBP and VDP, to strengthen and safeguard our systems, services and data.

Emerging Trends

40. The Government's personal data protection approach will need to evolve in tandem with technological changes, and the increasing use of digital tools in Government service delivery and operations. New use cases may require new approaches to data protection and management. For example, the Government will be publishing regular disclosure reports to help the public understand how personal data collected through TraceTogether and SafeEntry data have been used for purposes other than contact tracing[12].

41. A growing area of interest is the use of biometric data and the attendant data protection and security concerns. Biometric data has unique characteristics, such as being immutable, that set it apart from other types of personal data. The Government has therefore crafted additional guidelines to guide public agencies in using biometric data responsibly to discharge their functions, while safeguarding the data well. For example, stringent data security safeguards have been incorporated into the National Digital Identity Biometric Face Verification services, which enable users to transact with digital services from the public and private sectors. Security measures include the encryption of face scans and tagging of the images with anonymised identifiers, which are protected with tamper-evident logging. The Face Verification process also has safeguards to protect against impersonation fraud, e.g. application of liveliness detection technology that can detect the use of a photograph, video or mask during the verification process. Additionally, biometrics will not be used as the sole authentication factor for more sensitive transactions; other authentication factors (e.g. password, SMS-OTP, Singpass app may be required on top of biometrics).

---

12 The Disclosure Report will cover the use of TraceTogether data for purposes other than contact tracing from the date that legislative amendments were introduced in Parliament in Feb 2021.

42. Recent international incidents have highlighted the evolving nature of the threats in the cyber-space. In particular, ransomware attacks have become more sophisticated and have grown in scale. Locally, 89 ransomware cases were reported to SingCERT in 2020, a spike of 154% from the 35 cases reported in 2019[13]. Globally, there has been a seven-fold year-on-year increase in ransomware reports, with 2020 alone seeing a 311% increase in ransom amount paid as compared to 2019[14]. The impact from ransomware has also spilled over into the physical world with real-world consequences. For example, in early 2021, the cybercrime group DarkSide used ransomware in a double-extortion scheme on the Colonial Pipeline Company of the USA. In addition to the ransom demanded for the release of ransomware-locked systems, the hackers also threatened to release 100 GB worth of stolen data if they were not paid. The fuel supply interruptions arising from this incident had severe ramifications on the United States, even causing fuel shortages as panic buying set in[15].

43. These incidents and trends point to the need to constantly keep abreast of technological development and to always remain vigilant to potential areas of attack. The Government will continue to look into addressing ransomware threats by increasing data resilience and maintaining sufficient backups while ensuring that the threat surface to the data is properly managed.

---

13 Source: Singapore Cyber Landscape 2020

14 Source: Institute for Security and Technology Combating Ransomware Report (2021)

15 Source: Bloomberg, 2021. *Colonial Hackers Stole Data Thursday Ahead of Pipeline Shutdown.*

Conclusion

44. The Government will continue to digitalise and use data fully in our journey to transform Singapore into a Smart Nation. The Government has used data and digital tools extensively to aid our fight against COVID-19, which contributed significantly to Singapore's capabilities in managing the spread of COVID-19.

45. The increased storage, transfer and use of personal data will enlarge the potential surface area of attack that malicious actors can exploit. With the public sector using data more to serve the public, we must continue to ensure that the appropriate data protection safeguards are in place.

Annex A: Implementation Progress of the PSDSRC Initiatives

Of the 24 initiatives recommended by the PSDSRC have been implemented, 18 were implemented by 30 September 2020 (as planned) and as reported in the inaugural Update. 3 more initiatives have been implemented between 1 October 2020 and 31 March 2021 – these have been denoted with "New" in the Table below.

PSDSRC Initiatives		Timeline	Status as at 31 Mar 2021
Key Recommendation 1: Enhance technology and processes to effectively protect data against security threats and prevent data compromises.			
1.1	Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads	To be implemented from 2019 to 2023	Ongoing
1.2	Enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity	To be implemented from 2019 to 2023	Ongoing
1.3	Protect the data directly when it is stored and distributed to render the data unusable even if extracted	To be implemented from 2019 to 2023	Ongoing
1.4	Develop and maintain expertise in advanced technical measures	To be implemented from 2019 to 2023	*(New)* Implementation has started, and is ongoing
1.5	Enhance the data security audit framework to detect gaps in practices and policies before they manifest into incidents	By 30 Apr 2020	Implemented
1.6	Enhance the third-party management framework to ensure that third parties handle Government data with the appropriate protection	By 30 Apr 2020	Implemented

PSDSRC Initiatives		Timeline	Status as at 31 Mar 2021
Key Recommendation 2: Strengthen processes to detect and respond to data incidents swiftly and effectively.			
2.1	Establish a central contact point in the Government Data Office for the public can report Government data incidents.	By 30 Apr 2020	Implemented
2.2	Designate the Government Data Office to monitor and analyse data incidents that pose significant harm to individuals.	By 30 Apr 2020	Implemented
2.3	Designate the Government IT Incident Management Committee as the central body to respond to incidents with Severe impact.	By 30 Apr 2020	Implemented
2.4	Institute a framework for all public agencies to promptly notify individuals affected by data incidents with significant impact to the individual.	By 30 Apr 2020	Implemented
2.5	Established a standard process for post-incident inquiry for all data incidents.	By 30 Apr 2020	Implemented
2.6	Distil and share learning points with all agencies to improve their data protection policies/ measures and response to incidents.	By 30 Apr 2020	Implemented
Key Recommendation 3: Improve culture of excellence around sharing and using data securely, and raise public officers' competencies in safeguarding data.			
3.1	Clarify and specify the roles and responsibilities of key groups of public officers involved in the management of data security.	By 30 Apr 2020	Implemented
3.2	Equip these key groups with the requisite competencies and capabilities to perform their roles effectively.	Ongoing beyond 2021	Implementation has started and is ongoing
3.3	Inculcate a culture of excellence around sharing and using data securely.	Ongoing beyond 2021	Implementation has started and is ongoing

PSDSRC Initiatives		Timeline	Status as at 31 Mar 2021
Key Recommendation 4: Enhance frameworks and processes to improve accountability and transparency of the public sector data security regime			
4.1	Institute organisational Key Performance Indicators (KPIs) for data security.	By 30 Apr 2020	Implemented
4.2	Mandate that the top leadership to be accountable for putting in place a strong organisational data security regime.	By 30 Apr 2020	Implemented
4.3	Make the impact and consequences of data security breaches salient to public officers.	By 30 Apr 2020	Implemented
4.4	Ensure accountability of third parties handling Government data by amending the PDPA.	By 31 Oct 2020	(New) Implemented
4.5	Publish the Government's policies and standards on personal data protection.	By 31 Oct 2020	Implemented
4.6	Publish an annual update on the Government's personal data protection efforts.	By 31 Oct 2020	Implemented
Key Recommendation 5: Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime			
5.1	Appoint the Digital Government Executive Committee to oversee public sector data security.	By 31 Oct 2020	Implemented
5.2	Set up a Government Data Security Unit to drive data security efforts across the Government.	By 31 Oct 2020	Implemented
5.3	Deepen the Government's expertise in data privacy protection technologies through GovTech's Capability Centres.	By 31 Oct 2020	(New) Implemented

Annex B:
The Government's Data Incident Severity Classification

Data Incident Severity Classification	Impact of the incident
Very Severe	Exceptionally grave/ severe damage to national security, multiple government agencies or public confidence.
Severe	Serious damage to national security, one or more government agencies or public confidence. Death, serious physical, financial or sustained emotional injury or social stigma to an individual. Sustained financial loss to a business entity.
High	Some damage to national security, a government agency or public confidence. Temporary and minor emotional distress or disturbance to the individual. Reduction in competitiveness or a compromise of business interests.
Medium	Difficult or undesirable consequences to a government agency. Minor inconvenience to individual or businesses.
Low	Minimal impact on agencies, individuals or businesses.