THIRD UPDATE ON THE GOVERNMENT'S PERSONAL DATA PROTECTION EFFORTS

2022

SMART NATION & DIGITAL GOVERNMENT OFFICE

THIRD UPDATE ON THE GOVERNMENT'S PERSONAL DATA PROTECTION EFFORTS

Introduction

1. The Public Sector Data Security Review Committee (PSDSRC) was convened in March 2019 to review how the Government secures and protects 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. The PSDSRC published its report and recommendations in Nov 2019. 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 third update on the Government's efforts to safeguard personal data ("Update"). It outlines what the Government has done in the past financial year (FY2021) to strengthen the public sector data security regime.

Background

3. The number of data breaches reported globally continues to grow rapidly in recent years, with millions of individuals affected by data breaches[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. The pace of digital adoption has accelerated as the COVID-19 pandemic entered its second year in 2021. Many facets of everyday life, from workplace meetings to consumer activities, have moved from the physical domain to the digital space. As more data is created and exchanged, the risk of data being exposed or misused increases correspondingly. While technological developments create innovative ways to harness the value of data for economic or societal benefits, these same developments also pose new threats to data security.

5. These trends highlight the importance of the Government's continuous efforts to innovate and implement initiatives to safeguard personal data.

[1] Source: Identity Theft Resource Centre (ITRC) 2021 Annual Data Breach Report
[2] No. of complaints made to PDPC from 2019 to 2021 were as follows:
- Year 2019: 4,500
- Year 2020: 6,100
- Year 2021: 6,700

Trends in Number of Government Data Incidents Reported

6. There were 178 data incidents reported in FY2021, up from 108 in FY2020. This was a 66% increase in the total number of data incidents reported. The data incidents reported in the period from FY2019 to FY2021, broken down by the Government's incident severity classification[3], is as follows:

Total Number of Data Incidents Reported by Severity			
Data Severity Incident	**FY2019**	**FY2020**	**FY2021**
Low	33	64	126
Medium	37	44	52
High	5	0	0
Severe	0	0	0
Very Severe	0	0	0
Total	**75**	**108**	**178**

Table 1

7. The increase in reported data incidents is in line with global trends, as data use continues to proliferate in both the public and private sectors. Improved awareness amongst public officers on the need to safeguard data, and therefore report every incident no matter how minor, has also contributed to the increase.

8. Despite the increase, none of the 178 incidents reported in FY2021 were assessed to be of "High" severity or above. This demonstrates the continued downward trend in serious data incidents. 89% of the increase in FY2021, compared to FY2020, can be attributed to an increase in data incidents of "Low" severity. These are incidents that have been assessed to have minimal impact on individuals and businesses.

[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.

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 2). The Government accepted the PSDSRC's recommendations in full and committed to implement them by 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 2

Progress of implementing the PSDSRC's Recommendations

10. As of 31 March 2022, 21 of the 24 initiatives formulated to operationalise the five key recommendations have been implemented as planned (see Annex A for the detailed list of recommendations). The Government is on track to complete all 24 initiatives by end-2023.

11. Significant progress has been made on the remaining 3 initiatives (Recommendation 1.1 to 1.3) since the second Update was published in July 2021. These 3 initiatives, which are technical in nature, have been progressively implemented to protect data against security threats and prevent data compromises.

    a. The Central Account Management (CAM) solution is being implemented in phases to prevent unauthorised access to data by automatically disabling user accounts that are no longer needed.

    b. A suite of Data Loss Protection tools is being rolled out to prevent the loss of sensitive data from the Government Network and Devices by using technical and process controls to automatically detect risky user behaviour.

    c. The Data Privacy Protection Capability Centre (DPPCC), established on 31 December 2020, has been developing and deploying advanced data

protection toolkits based on advanced privacy-enhancing technologies, such as differential privacy techniques, to protect Government data.

12. 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.

Highlights of Government's Initiatives to Strengthen Data Security from 1 April 2021 to 31 March 2022

13. The Government's efforts in strengthening data security in FY2021 were centred on the five desired outcomes (Table 2) of a robust data security regime.

Outcome 1: Protect Data and Prevent Data Compromises

14. The Government has continued to build on the PSDSRC-recommended technical and process measures to protect data and minimise the risk of data compromises (Recommendations 1.1 to 1.3). These technical and process measures have been incorporated into Government Instruction Manuals and public agencies have progressively implemented these measures into their processes and operations to safeguard government data against security threats.

15. The impact of potential data compromises has been mitigated through technical and process measures. For example, the technical measure of masking sensitive data when stored or distributed limits the impact should the masked data be exposed inadvertently. In one of the data incidents reported in FY21, documents containing personal data were mistakenly uploaded onto a government portal due to misconfiguration in the web application server. Fortunately, as the personal data was masked, the impact of the data incident was minimal.

16. The Government has made progress on the implementation of the complex technical solutions recommended by the PSDSRC (Recommendation 1.1-1.2), to further strengthen the public sector's data security posture.

17. In August 2021, the Government began the development of Central Accounts Management (CAM) solution to prevent unauthorised access to data and potential data incidents through greater automation. The CAM solution seamlessly integrates Human Resource (HR) processes with access rights to operational IT systems. When officers leave the organisation, CAM automatically removes and disables their user accounts from the organisation's operational IT systems. This in turn prevents either unauthorised access by officers who have left their roles or the exploitation of dormant accounts by malicious actors.

18. The CAM solution also addresses the redeployment of officers within the same organisation. Such staff movements and changes of job portfolios often require officers to have different access rights in operational IT systems. CAM will automatically trigger notifications to review officers' access rights in light of their redeployment. Such reviews ensure that officers are given the appropriate access to only data that is relevant to their immediate work and minimises the risk of unauthorised data access. In addition, the solution triggers notification to agencies to review user's access rights due to officer changing portfolios. This is in line with the Government's principle of least privilege, allowing officers only sufficient access to perform the required job.

19. The CAM solution was commissioned in April 2022. Given the high number of systems to onboard, the integration of Government IT systems to CAM is in

progress. As of 1 April 2022, 32% of eligible Government IT systems have been configured for onboarding to CAM solution. These include central systems used by all public officers, such as the Whole-of-Government collaboration and productivity platform, and key systems used by officers handling Government's transactions with third-party vendors. The onboarding of remaining systems is due to be completed by end-2023.

20. The Government progressively deployed the Whole-Of-Government (WOG) Data Loss Protection (DLP) tools to prevent accidental loss of sensitive data from Government networks, systems and devices. WOG DLP tools use technical and process controls to detect risky user activities. Upon detection, the DLP tools will prompt the user to take certain actions, such as acknowledging that the data was intended to be transferred before proceeding to do so or stop the anomalous data transfer altogether to prevent any loss of data.

21. As of 31 March 2022, the WOG DLP tools have been deployed to the WOG email service and secure internet surfing gateway. The WOG DLP tools will be subsequently deployed to WOG laptops in August 2022.

Outcome 2: Detect and Respond Swiftly to Data Incidents

22. Even with the implementation of a suite of technical and process measures to prevent data compromise, it is not possible to eliminate data incidents altogether. Hence, when a data incident occurs, we need to be able to detect and respond swiftly.

23. 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. The GDSCC is intended to augment the Government's capabilities to detect data incidents and provide a convenient channel for the public to report potential data incidents.

24. In FY2021, the GDSCC received 101 reports, of which 14 were classified as "Data Incidents" upon further investigation:

No. of Data Incidents Reported through GDSCC	
Incidents Reported	**FY2021**
Incidents classified as "Data Incidents" upon further investigation	14
Incidents not classified as "Data Incidents"	87[4]
Total Incidents Reported to GDSCC	101

Table 3

[4] 87 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 teams to handle.

All incidents and queries were resolved in a timely manner, and in accordance with established service standards, as shown in Table 4 below.

Categories	Definitions	Required Response Time	No of queries
Simple	Simple cases refer to straightforward queries with information ready	Within 3 working days	73
Standard	Standard cases refer to cases which require some investigation by the affected agency	Within 10 working days	3
Complex	Complex cases refer to cases which require significant investigation, and may have cross-agency involvement	Within 15 working days	25
Total			**101**

Table 4

25. Preparation and exercises are key to maintaining incident response capabilities. The Government conducted the inaugural Central ICT and Data Crisis Management Exercise (CMX) involving a total of 33 Agencies across 5 Ministries in September 2021. The exercise scenarios included prevalent threats such as supply chain attacks and ransomware leading to disruption of services. The CMX exercised the Government's ability to provide a coordinated response and tested the capabilities of agencies to respond effectively.

26. The public agencies that did not participate in the central ICT and Data Incident Management exercises carried out their own cyber and data security incident exercises. These served to simulate data incidents and test the readiness of agencies to contain and manage the impact of such incidents.

27. These annual exercises provide an opportunity for participants to understand their roles and responsibilities in the swift detection and response to data incidents. The experience enhanced officers' competencies and readiness in managing different types of government incidents.

Outcome 3: Competent public officers embodying a culture of excellence

28. Data security is an ongoing journey and requires the continuous education of public officers. To that end, 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.

29. Since May 2021, the Government ran a series of engagement campaigns to engage all public officers on the role they play in ensuring data security and safeguarding government data. Engagement activities include Data Security virtual roadshows to raise awareness and send the message of 'Using Data

Securely' to officers. Digital content was also disseminated on various government digital platforms to share practical steps and enable officers to proactively incorporate data security measures into their work processes.

30. In July 2021, a series of 'Train-the-trainer' data security workshops was rolled out to equip agencies with the skills and resources to develop their internal engagement plans effectively. With a public service of over 150,000 officers, such internal engagements are critical to building and maintaining the culture of excellence in using data securely.

31. The latest edition of the Data Security e-learning module[5] was refreshed in early 2022 to include new content on the latest policies and measures that officers should adopt in their daily work. Given the increase in remote work, best practices such as the secure use of virtual conferencing platforms were emphasised.

32. Instilling a culture of excellence is a long-term endeavour and will require sustained efforts across many years at all levels of the organisation, particularly for a large organisation such as the Public Service. We will continue to develop our people's capabilities and instincts in managing and securing data.

Outcome 4: Accountability for data protection at every level

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

34. Beyond the measures introduced at a Whole-of-Government level to ensure data security, the Government has also worked to ensure a high data protection standard as public agencies continued to collect and use data to serve Singaporeans better. Government agencies take a data minimisation approach, collecting and using only data which is required for our objectives and intent. In addition, at each specific instance of collection and use, the Government ensures proper data protection procedures and safeguards, to ensure citizens' data are managed in a responsible manner (see Boxes 1 and 2 for examples).

Box 1: Issuance of digital birth and death certificates in place of physical certificates from 29 May 2022, with improved authentication and fraud prevention

The birth and death registration processes has been made simpler, and digital birth and death certificates have been issued in place of physical certificates from 29 May 2022. This is part of the Government's ongoing effort to streamline and digitalise services to serve citizens better. Parents of newborns and next-of-kin of the deceased will be able to conveniently

[5] 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.

download and store the digital certificates on their personal mobile devices and laptops.

The digital certificates are official and legal documents issued by the Immigration & Checkpoints Authority (ICA). Data protection and privacy measures are put in place to prevent data loss or theft, unauthorised access and disclosure. For example, parents who are Singpass users and who wish to retrieve their child's digital birth certificate will be required to log in using Singpass, which requires two-factor authentication (2FA). All information will be stored and secured in the government database.

The digital certificates allow for greater data protection as they provide additional means of verification which is not possible with physical certificates. QR codes included on the digital certificates may be scanned by both government agencies and private entities, e.g. financial institutions to ensure the authenticity of the certificate. Personal data is also better managed as institutions requiring proof of birth can simply verify an authentic digital birth certificate instead of asking for duplicates to be submitted in hard copy.

Box 2: Option to launch Singpass app with masked Digital IC so as to preserve data privacy

The Digital IC is a digitised document of an individual's identity, complete with personal information such as their name, identification number, photograph, date of birth and other pertinent details.

It can be accessed via the Singpass mobile application and serves as a way for business owners and organisations to have a secure and convenient means of in-person identity verification.

Several security and privacy features are built into the Singpass application to allow users to customise whether the Digital IC are shown or hidden by default. Even if the Digital IC is shown by default, only the individual's photo and last four characters of NRIC number are displayed to shield full personal information. Further authentication is required to display full NRIC details. These features ensures that personal information is shielded until further authentication is requested.

Outcome 5: Sustainable and resilient data security regime

35. 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.

36. Since its establishment, the DPPCC has been developing data privacy protection toolkits based on advanced privacy enhancing techniques. These techniques, when applied to a dataset, aim to preserve privacy while still allowing for effective use of data. The toolkit will be tested and iteratively improved for widespread adoption by agencies.

37. In addition, the DPPCC has been working with agencies to drive solutions for strengthening data privacy and protection for key systems. These solutions include dataset segregation and stringent standards of encryption to reduce the risk of data exposure.

What's Next

Lessons from the Data Incidents and Data Security Initiatives

38. The Government's initiatives have helped to improve the public sector's data security posture. The technical and process measures put in place by PSDSRC recommendations have minimised the impact of data incidents.

39. The Government takes a serious view of data incidents. Officers found responsible have been counselled, and where required, officers have also been disciplined, with penalties ranging from formal reprimands to financial penalties.

40. The implementation of CAM solution and WOG DLP Tools will add an important basic line of defence against data compromises. We will also continue our effort to engage public officers to increase data security awareness and knowledge.

41. Beyond that, we will continue to work with the cybersecurity and data security community through programmes such as the GDSCC and CMX to strengthen and safeguard our systems, services and data.

Emerging Trends

42. While the Government continues to develop a comprehensive a data security regime against current threats, we must also respond to emerging trends and threats.

43. Scams are a perennial problem. Scammers exploit digital technologies to operate at a global scale and their tactics have become more sophisticated by the year. The reported cases of scams have risen from 15,651 cases in 2020 to 23,931 in 2021[6]. In particular, phishing scams which trick victims into disclosing their personal data demonstrate the devastating consequences of not protecting data.

44. The Government is leveraging technology to detect scams more effectively. One example is ScamShield, a mobile app that filters potential scam messages and blocks scam calls using trained Artificial Intelligence (AI) models. Government

[6] Source: SPF Annual Crime Brief 2021

agencies, together with private sector stakeholders, are also exploring the use of enhanced fraud surveillance systems based on AI to flag suspicious transactions and identify possible fraudulent behaviour in real-time. Combatting scams needs a whole of society effort, the Government will continue to work with private sector partners to coordinate efforts to raise collective awareness in the fight against scams.

45. Another emerging trend is the accelerated adoption of digital wallets which store digital documents such as virtual vaccination cards or digital IDs. Digital wallets allow users to store verified information relating to the user's identity and other credentials from multiple issuers. The user will then have greater control over which identity or data attributes they wish to share. For example, users can prove a specific personal attribute, such as age, without revealing their identity or other personal details.

46. Today, the Singpass Document Wallet allows users to access government-issued documents within their profile. An initial use case of the Document Wallet is storing of the Vaccination HealthCert from Notarise Portal. Users can present their HealthCert via the Singpass Document Wallet to immigration authorities to facilitate cross-border travel. More document types will be added to the Singpass Document Wallet in future.

47. These trends point to the increasing value of data and the corresponding risk that criminal elements will exploit data for malicious purposes. There is thus a need for the Government to keep abreast of such developments and put in place measures to protect data. The Government will continue to address these threats by investing in technology and through citizen engagement.

Conclusion

48. The Government will continue to leverage data and new technologies to drive broader efforts to build a digital economy and digital society, in support of our Smart Nation ambitions.

49. Data is key for digital transformation, and public agencies will continue to use data to make life better for citizens and businesses. However, such extensive storage, transfer and use of personal data and digital tools also increase the potential areas of attack. Hence the Government will continue to enhance our protection efforts to safeguard the data of both citizens and businesses.

Annex A: Implementation Progress of the PSDSRC Initiatives

Of the 24 initiatives recommended by the PSDSRC have been implemented, 18 were implemented by 30 Sep 2020 (as planned) and 3 more initiatives have been implemented between 1 Oct 2020 and 31 Mar 2021. Implementation of the technical measures (Recommendations 1.1-1.3) to protect data against security threats and prevent data compromises are ongoing.

PSDSRC Initiatives		Timeline	Status as of 31 Mar 2022
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	Continual Effort beyond 2023	Implementation has started and will be continuous beyond 2023
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
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.			

PSDSRC Initiatives		Timeline	Status as of 31 Mar 2022
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.	Continual Effort beyond 2023	Implementation has started and will be continuous beyond 2023
3.3	Inculcate a culture of excellence around sharing and using data securely.	Continual Effort beyond 2023	Implementation has started and will be continuous beyond 2023
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	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	Implemented

Annex B: The Government's Data Incident Severity Classification

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.