SMART NATION
&
DIGITAL GOVERNMENT OFFICE

UPDATE ON THE GOVERNMENT'S PERSONAL DATA PROTECTION EFFORTS

2023

The publication of this document is for the information of the public. The enclosed facts, statistics and analyses are based on information available at the time of publication. The contents of this publication are provided on an "as is" basis without warranties of any kind. The Government will not be liable for any loss or damage of any kind caused as a result (direct or indirect) of the use of the publication, including but not limited to any damage or loss suffered as a result of reliance on the contents contained in the publication. The Government reserves the right to refine its analyses as further information is made available.

UPDATE ON THE GOVERNMENT'S FY2022 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 end-to-end, as well as 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 November 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 (heretofore referred to as the "Update") outlines the efforts undertaken by the Government in FY2022 to safeguard personal data and strengthen the public sector data security regime.

Background

3. In Singapore, the number of complaints made to the Personal Data Protection Commission (PDPC) on potential personal data breaches by private organisations decreased by 46%[1] from the previous year.

4. The decrease in the number of complaints is within expectations as Singapore emerges from the COVID-19 pandemic. While the increase in the number of complaints in 2020 and 2021[2] were likely to be due to the rapid pace of digitalisation due to COVID-19, the recent decrease in the number of complaints made to the PDPC highlights the Government's continuous efforts to innovate and implement initiatives to safeguard personal data.

5. In the face of greater digitalisation and even new technological developments like Generative Artificial Intelligence (AI), data security will continue to be a key national priority. These trends emphasise the need for the Government to continuously invest in improving our security posture.

[1] The Personal Data Protection Committee's (PDPC) Enquiry and Complaint Figures *(2022) show that the no. of complains made to the PDPC for the past three years is as follows:*

- 2020: 6,100
- 2021: 6,700
- 2022: 3,600

[2] Personal Data Protection Committee's (PDPC) Enquiry and Complaint Figures *(2022)*

Trends in Number of Government Data Incidents Reported

6. There were 182 data incidents reported in FY2022, an increase of 2% from the 178 incidents reported in FY2021. The data incidents reported in the period from FY2019 to FY2022, broken down by the Government's incident severity classification (see Annex A for details on the classification framework), is as follows:

Total Number of Data Incidents Reported by Severity				
Data Severity Incident	**FY2019**	**FY2020**	**FY2021**	**FY2022**
Low	33	64	126	136
Medium	37	44	52	46
High	5	0	0	0
Severe	0	0	0	0
Very Severe	0	0	0	0
Total	**75**	**108**	**178**	**182**

Table 1

7. None of the incidents reported in FY2022 were assessed to be of "High" severity or above. This marks the third year in a row with no incidents of "High" severity and above. As compared to FY2021, there was a 12% decrease in the number of data incidents of "Medium" severity, that pose difficult or undesirable consequences to a Government agency or which pose minor inconvenience to individuals or businesses.

8. While the majority of FY20222 data incidents were of "Low" severity, i.e. incidents that have been assessed to have minimal impact on agencies, individuals, or businesses, the Government takes a serious view on any increase in data incidents. The slight increase in FY2022 data incidents is likely due to the acceleration of data-sharing amongst agencies as we return to normalcy post-COVID and continue to push our digitalisation efforts. In addition to improving awareness amongst public officers on the need to safeguard data, technical measures to improve our data security posture will also be implemented.

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-FY2023[3].

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 2023, 22 of the 24 initiatives formulated to operationalise the five key recommendations have been implemented as planned (see Annex B for the detailed list of recommendations). The Government is on track to complete the implementation of all 24 initiatives by the end of FY2023.

11. For the period from April 2022 to March 2023, the Government has done the following to improve upon the five desired outcomes:

a) <u>Protect data and prevent data compromises</u>: the Government has enhanced security measures to protect data and prevent data compromises;

b) <u>Detect and swiftly respond to data incidents</u>: the Government has continued to encourage the prompt reporting of data incidents by public officers; the Government has also continued to respond to data

[3] *The implementation timeline for PSDSRC recommendations has been aligned with the reporting of data incidents and the Government's personal data protection efforts.*

incidents and queries in a timely manner in line with existing service standards;

c) Develop data security competencies among public officers: the Government has continued to engage public officers and update their knowledge on data security;

d) Ensuring accountability for data protection at every level: the Government has continued to monitor adherence to our data protection frameworks and processes; and

e) Building a sustainable and resilient data security regime: the Government has developed tools to ensure that data security posture is further strengthened.

12. These efforts continue to strengthen the Government's capabilities to safeguard data, amidst an increasingly complex operating 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) Enhanced efforts in implementing data protection capabilities, such as with the implementation of the Whole-of-Government (WOG) Data Loss Protection (DLP) tool.

13. In FY2022, the Government also completed the implementation of PSDSRC Recommendation 1.2 to "enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity". This was achieved by:

a) Maintaining data lineage to support data incident management;
b) Digitally watermarking files to identify the files' originator;
c) Providing enhanced logging and active monitoring of data access to detect anomalous activities and support remediation when data incidents occur; and
d) Alerting public officers that they are communicating classified and/or sensitive information to lower the likelihood of accidental or unauthorised disclosure through email.

Highlights of Government's Initiatives to Strengthen Data Security from 1 April 2022 to 31 March 2023

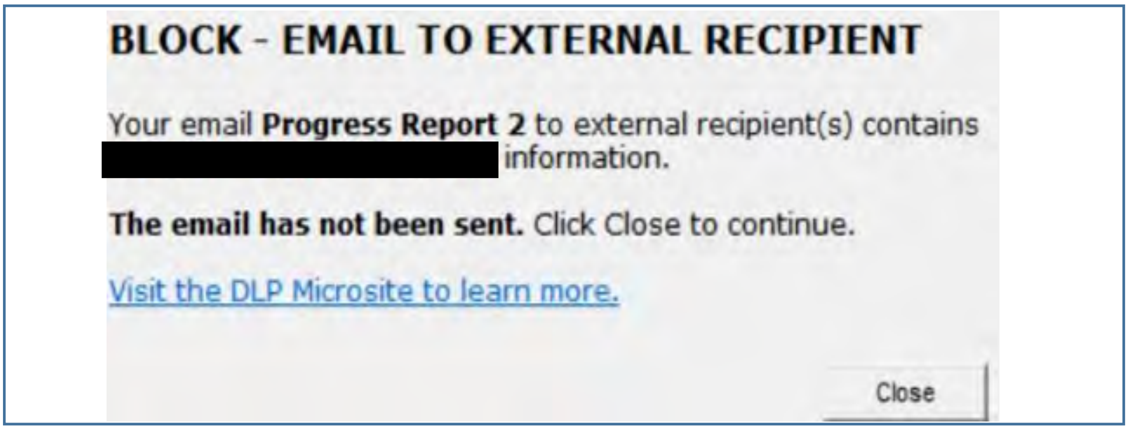
14. In FY2022, the Government has continued to focus on attaining the five desired outcomes described in Table 2 as part of our efforts to strengthen data security.

Outcome 1: Protect Data and Prevent Data Compromises

15. 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. For example, under Recommendation 1.1 to "reduce the surface area of attack by minimising data collection, data retention, data access and data downloads", the development of a Central Accounts Management (CAM) solution has helped to improve data access control by promptly removing expired access rights to prevent potential data compromises.

16. As of 1 April 2023, 63% of eligible Government IT systems have been onboarded to the CAM solution. The adoption of the CAM solution allows agencies to automate access control reliably, efficiently, and effectively, thereby mitigating the risks of unauthorised access by officers who have left their roles and the exploitation of dormant accounts by malicious actors.

17. To fulfil PSDSRC Recommendation 1.2 to "enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity", the Government has also deployed the WOG DLP tool in FY2022 to all Government laptops to prevent the accidental loss of classified and/or sensitive data from Government networks, systems, and devices. The WOG DLP tool has controls that detect and highlight risky user actions to prevent accidental data loss and improve data hygiene practices. For instance, the tool blocks public officers from sending information that could cause serious damage to national security or interests to external parties. It also reminds public officers to check that they have sent the correct file to the intended recipients. The pictures below (Figure 1 to 2) illustrate how the WOG DLP tool functions.



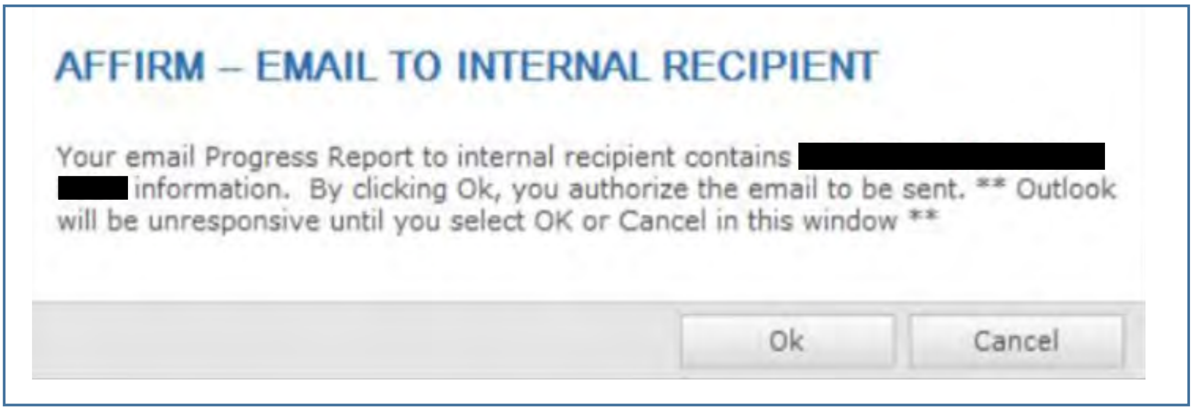
BLOCK - EMAIL TO EXTERNAL RECIPIENT

Your email **Progress Report 2** to external recipient(s) contains [redacted] information.

The email has not been sent. Click Close to continue.

Visit the DLP Microsite to learn more.

Figure 1: The WOG DLP tool's "BLOCK" function prevents public officers from sharing certain classified materials to external parties.



AFFIRM – EMAIL TO INTERNAL RECIPIENT

Your email Progress Report to internal recipient contains [redacted] [redacted] information. By clicking Ok, you authorize the email to be sent. ** Outlook will be unresponsive until you select OK or Cancel in this window **

Figure 2: The WOG DLP tool's "AFFIRM" function reminds public officers to confirm that they intend to send classified information to stated recipients, thereby mitigating the risk of unintended data exposure.

<u>Outcome 2: Detect and Respond to Data Incidents</u>

18. The Government Data Security Contact Centre (GDSCC) was established in April 2020 to augment the Government's capabilities to detect data incidents and to act as a public reporting channel. This was done to encourage the reporting of Government data incidents by members of the public. GDSCC capabilities also ensure that we are able to respond swiftly to data incidents and take the necessary steps to remediate the situation.

19. In FY2022, the GDSCC received 70 reports, all of which were resolved in a timely manner. Of the 70 reports, 20 were classified as "Data Incidents" upon further investigation:

No. of Data Incidents Reported through GDSCC	
Incidents Reported	**FY2022**
Incidents classified as "Data Incidents" upon further investigation	20
Incidents not classified as "Data Incidents"	50
Total Incidents Reported to GDSCC	70

Table 3

20. Preparation and exercises are key to maintaining incident response capabilities. The annual Central ICT and Data Crisis Management Exercise (CMX) was held from August to September 2022 and involved a total of 24 public agencies across five Ministries. The exercise scenarios included prevalent threats, such as ransomware and loss of services due to power outages to critical infrastructure. Exercises such as CMX allow agencies to build capabilities that ensure a coordinated and effective response should the need arise.

21. Besides the 24 agencies that participated in the FY2022 CMX, the remaining public agencies carried out their own cyber and data security incident exercises. These exercises simulated data incidents, tested the agencies' readiness to contain and manage the impact of such incidents, and helped them to better understand their roles and responsibilities in the event of a cyber or data security incident.

Outcome 3: Competent public officers embodying a culture of excellence

22. In this past year, the Government has continued to enhance public officers' awareness on data security and to instil in every public officer a culture of excellence in using data securely. Today, public officers are generally well-equipped to protect the data that they collect and use.

23. In FY2022, the Government continued to conduct engagement campaigns to engage public officers on the role they play in ensuring personal data protection in safeguarding Government data. The campaigns included workshops that focused on providing practical steps to prevent personal data loss. The practical advice was tailored to agencies' specific use cases and were designed to enable public officers to incorporate personal data protection measures into their work processes.

24. The annual e-learning programme was launched on 8 May 2020 as one of the recommendations by the PSDSRC. As part of the Government's commitment to ensure that public officers are kept abreast on data security matters, the latest edition of the Data Security e-learning module was refreshed on 22 February 2023 to include new content on the latest policies and measures that public officers are to adopt in their daily work. The e-learning module was enhanced to emphasise the importance of personal data and data loss protection. In addition, more questions pertaining to data classification were included to improve public officers' understanding and application of classification guidelines.

25. All officers are required to complete the Data Security e-learning module, including an accompanying quiz and a declaration that they have understood their responsibilities and liabilities in handling Government data, annually. New hires are to complete the module within three months of joining the public agency. The Government recognises that instilling a culture of excellence among public officers is a task that is ongoing and requires long-term effort at every level of the public service.

Outcome 4: Accountability for data protection at every level

26. The Government has continued to enhance the frameworks and legislative measures to hold leaders, individuals, and organisations accountable for protecting Government data.

27. Beyond the measures introduced at the WOG level to ensure data security, the Government has also continued to ensure a high data protection standard as agencies continue to collect and use data to serve Singaporeans better. A data minimisation approach continues to be our default: meaning that agencies do not collect and use more data than which is necessary. In addition, the Government ensures that proper data protection procedures and safeguards are adhered to whenever data is collected and implemented to ensure that citizens' data is managed responsibly.

28. The Government also continually strives to improve its data protection measures at every level. Over the past year, the Government has taken steps to further tighten its data protection policies and processes. For example, one initiative has been to improve public officers' competencies in the area of personal data protection. As part of the Basic Digital Literacy competency programme for the public sector, public officers underwent the Cybersecurity and Data Protection Courseware, which featured a new section dedicated to personal data protection issues, to improve public officers' management of citizens' personal data.

Outcome 5: Sustainable and resilient data security regime

29. To keep up with emerging threats and new technologies, the Government established the Data Privacy Protection Capability Centre (DPPCC) on 31 December 2020. In order to raise the Government's capabilities and expertise in data privacy protection technologies, the DPPCC launched the inaugural Central Privacy Toolkit in March 2023. It is a one-stop self-service portal that helps public officers apply privacy enhancing techniques to datasets while preserving the data's value for sharing and exploitation.

30. The Central Privacy Toolkit enables public officers, including non-technical users, to implement end-to-end anonymisation workflows based on Government and sector-specific policy requirements. By accessing the toolkit on a self-help portal, public officers will now find it easier to anonymise datasets in a standardised and secure manner. This will enable them to share data within and outside of the public sector more rapidly, confidently, and securely, thereby mitigating the risk of data leaks that stem from sharing datasets.

31. To date, public officers from over 80 agencies have used the Central Privacy Toolkit to improve the data security and privacy of their datasets, while reducing re-identification risk. DPPCC will continue to work with agencies, academics, and industry partners to prototype new forms of privacy enhancing technologies, such as synthetic data generation and differential privacy. These

technologies will be deployed and integrated into key systems and democratised to support diverse Government use cases.

What's Next

Lessons from the Data Incidents and Data Security Initiatives

32. The Government remains vigilant and invested in encouraging good data protection practices by the public sector. This is an ongoing effort that requires every single officer to be equipped with knowledge and the right tools to protect data.

33. The use of technology is key to promulgating the safe and secure use of data. The development and implementation of the Central Privacy Toolkit shows that leveraging technology can reduce public officers' effort in securing data and empower them through self-service tools. Previously, public officers had to work with technically trained personnel to anonymise data for sharing. Now, with the toolkit, public officers can anonymise data on their own through the self-service portal. This highlights the Government's effort to innovate solutions that empower public officers to carry out their data protection responsibilities with ease.

34. Through the WOG DLP tool's implementation, we also learnt that security measures must be balanced with user-experience to achieve our outcomes while not constraining data use by officers. Measures, such as alerting officers to risky actions, could lead to user desensitisation if the alerts are voluminous. The Government remains committed to continuously refining the WOG DLP tool to reduce user burden, maintain public officers' productivity, while striving to enhance the Government's security posture.

35. Following various training programmes and workshops conducted in the past financial year, the Government will press on with a robust engagement and education strategy. Such sessions ensure that public officers not only comply with guidelines but also understand the intent of data policies and serve to develop their capabilities in maintaining data security.

Emerging Trends

36. The past year saw the proliferation of Artificial Intelligence (AI) and commercial Large Language Model (LLM) applications such as ChatGPT and GPT-4. These can power a wide range of applications, such as generating text responses to questions. While this technology brings significant value and productivity gains for public officers, they also carry data security risks for the Government.

37. The Government is keeping up with advancements in AIs and LLMs while concurrently developing guidelines to ensure its responsible use. New guidelines on the use of LLM applications within the public sector were rolled out in May 2023. The Government has set up guardrails on the type of

information that can be input into LLM applications. This provides guidance to public officers on the proper use of LLM applications to prevent accidental data loss. The Government is also making a continuous effort to explore potential measures to minimise risks of data leaks, such as the ability to detect and prevent the input of sensitive information into LLM applications.

Conclusion

38. The Government recognises that the journey to strengthen data protection measures is an ongoing one. As technology advances, so too will the data security risks and mitigation opportunities evolve. We will therefore continuously scan the horizon for new capabilities to strengthen our data protection measures in the face of this rapidly changing technological landscape.

39. The Government has adopted a resilient mindset and remains ready to adapt to novel technological developments, such as the emergence of LLMs. We remain committed to identifying new threats posed by such developments and to address them in a timely fashion, meeting the objective of safeguarding Government data as our top priority.

Annex A: 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.

Annex B: Implementation Progress of the PSDSRC Initiatives

Of the 24 initiatives recommended by the PSDSRC, 22 have been implemented as of 31 March 2023. The implementation of the two remaining technical measures (Recommendations 1.1 and 1.3) to protect data against security threats and prevent data compromises are ongoing.

PSDSRC Initiatives		Timeline	Status as of 31 Mar 2023
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	By 31 Mar 2024 (By end FY2023)	Ongoing
1.2	Enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity	By 31 Mar 2023	Implemented
1.3	Protect the data directly when it is stored and distributed to render the data unusable even if extracted	By 31 Mar 2024 (By end FY2023)	Ongoing
1.4	Develop and maintain expertise in advanced technical measures	Continual effort beyond FY2023	Implemented
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 2023
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 FY2023	Implemented
3.3	Inculcate a culture of excellence around sharing and using data securely.	Continual effort beyond FY2023	Implemented
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 that can meet future needs			
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