ANNUAL UPDATE ON

THE GOVERNMENT'S PERSONAL DATA PROTECTION EFFORTS 2020

SMART NATION
&
DIGITAL GOVERNMENT OFFICE

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.

Introduction

1 Data is a valuable asset that can bring about tremendous opportunities for individuals and societies. It has the potential to improve lives and strengthen communities. While the Government uses a wide range of data, including personal data, to serve citizens, it must do so in a manner that ensures the information is secured. Failure to safeguard sensitive data can lead to serious harm to individuals and/or national security.

2 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 personal data protection efforts to provide the public with greater visibility over its approach to data security and data protection.

3 This publication is the first annual update on the Government's personal data protection efforts. It outlines what the Government has done in the past year (up to 30 Sep 2020) to strengthen the protection of personal data and the public sector data security regime. This is vital as we use data more extensively to formulate better policies, deliver more personalised services and optimise operations.

Background

4 The number of data breaches globally has been growing rapidly in recent years. The total number of records exposed in 2019 is almost 300 percent more than in 2018[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]. These trends highlight the increased data security risks faced by the private and public sectors and the importance and urgency of implementing the necessary safeguards to protect personal data.

5 To enhance the public sector data security regime, the PSDSRC made five key recommendations based on five desired outcomes:

[1] "In 2019, a total of 7,098 reported breaches exposed 15.1 billion records," Help Net Security, 11 February 2020, Source: https://www.helpnetsecurity.com/2020/02/11/2019-reported-breaches.

[2] No. of complaints made to PDPC from year 2017 to year 2019 (Source: PDPC website)

	Year 2017	Year 2018	Year 2019
No. of Complaints to PDPC	2,200	2,700	4,500

Note: New NRIC requirements prohibiting private organisations from collecting NRIC by default came into effect in October 2019.

Desired Outcomes	Key Recommendations
Protects data and **prevents** data compromises	1. Enhance technology and processes to effectively protect data against security threats and prevent data compromises.
Detects and responds 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 manner	5. Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime that can meet future needs.

Table 1

6 The Government accepted the PSDSRC's recommendations in full and committed to implementing them in phases from 2020 to 2023. In Budget 2020, the Government announced that it would invest $1 billion over the next 3 years to enhance cybersecurity and data security in the public sector[3].

7 In 2020, the Government focused its data security efforts on implementing the recommendations made by the PSDSRC. Of the 24 initiatives formulated to operationalise the five key recommendations, 18 have been implemented as of 31 Oct 2020. (More information on these initiatives is in the section, "Highlights of the Government's Initiatives to Strengthen Data Security in 2020".) 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; and
f. Improved transparency of the public sector data security regime.

Highlights of Government's Initiatives to Strengthen Data Security in 2020

8 The Government's initiatives and efforts in data security in 2020 were centred on the five desired outcomes (Table 1) of a robust data security regime.

[3] Singapore Budget 2020 Speech, Source: https://www.singaporebudget.gov.sg/budget_2020/budget-speech/d-sustaining-singapores-success-for-our-future-generations

Outcome 1: Protect Data and Prevent Data Compromises

9 The Government implemented technical tools and instituted changes in work processes to minimise the risk of data compromises.

10 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.

11 These tools have already proven useful. In November 2019, the email data protection tool detected a data incident at the Singapore Accountancy Commission and stopped further unauthorised disclosure of data (see Box 1).

Box 1: Detecting an unintentional data disclosure by the Singapore Accountancy Commission.

Over the period from June to October 2019, an officer from the Singapore Accountancy Commission (SAC) unknowingly attached a file containing personal information of 6,541 individuals (e.g. contact details and examination results) in emails that were sent to 41 people in 22 organisations.

The unintended data disclosure was uncovered by the email data protection tool that was implemented in October 2019, as the tool alerted the email sender that the email contained sensitive data. SAC immediately rectified the mistake and prevented further unauthorised disclosure of the data. SAC also convened a committee to inquire into the incident and make recommendations to improve the organisation's personal data protection practices.

After a review of the incident, SAC took appropriate disciplinary actions against the officers and supervisors involved, in the form of penalties ranging from formal warning letters to financial penalties of up to half-month pay.

12 The Government is preparing for the implementation of other technical measures, some of which require significant re-architecting of technical systems (see Box 2 for two examples of the key technical measures). These tools will also help to address several of the findings highlighted by the Auditor-General's Office, such as weak IT controls and poor review of user / privileged access to IT systems containing sensitive data.

Box 2: Data Loss Prevention and Central Accounts Management

The Government is developing a Whole-of-Government (WOG) Data Loss Prevention (DLP) programme to prevent the loss of sensitive data from endpoint devices, networks and ICT systems. The DLP programme will focus on addressing common causes of data incidents in the public sector such as the unintentional transfer of documents containing sensitive data during bulk data transfers. The DLP programme will use a combination of technical and process controls to detect risky user actions that might result in data loss and guide the users to take the appropriate actions. For example, when a public officer attempts to copy sensitive data out from the laptop using authorised storage media, the DLP tool will highlight this risky activity and require the officer to affirm the action before proceeding.

We expect to complete the implementation of the WOG DLP programme by end-2021.

Concurrently, the Government is also developing a Central Accounts Management Programme where technical solutions are used to automate the process of removing and granting systems access for officers in more than 2,000 IT systems across Government. Controlling access to IT systems is a key step to ensure that only authorised users have access to the sensitive data stored in IT systems. This programme is intended to reduce the need for manual adjustments to access controls, which can be prone to human errors. This programme will address several of the findings by the Auditor-General on the weak IT access controls and the need to detect and remove user / privileged accounts that are no longer needed, to ensure that there is no unauthorised use or access of data[4].

We expect to complete the implementation of the Central Accounts Management programme for about 800 high priority systems, based on data security risk, by end-2023. We will expand the programme to cover the remaining systems by end-2024. In the interim, we have made available a solution which will alert agencies to staff movements and role changes so that agencies can manually remove the user accounts that are no longer required, in a timely manner.

Box 3: Protecting user data in the TraceTogether Programme

The foundation laid by the PSDSRC recommendations has given us the confidence to rapidly implement new digital contact-tracing tools such as TraceTogether, while ensuring that individuals' personal data collected through these solutions would remain well-protected. The Government's data protection principles and relevant PSDSRC initiatives were incorporated into the design of these tools from the onset.

The TraceTogether Programme comprises an App and Token which use BlueTooth technology to identify people who have been in close proximity with the infected person.

[4] In the FY2019/20 Auditor General's Office report, 6 public agencies were found to have weak IT controls in the area of securing user and privileged access for some of their IT systems.

The TraceTogether App and Token have been designed with personal data protection in mind. The relevant PSDSRC measures have been implemented in the infrastructure to safeguard TraceTogether users' data.

For example, only the necessary data is collected – TraceTogether collects proximity data to identify potential close contacts of a COVID-19 patient. The proximity data collected by the App or Token is stored in the device in an encrypted format. In the event the App or Token is compromised, the attacker will not be able to identify the users or their close contacts.

Stringent measures have also been put in place to ensure that only authorised public officers have access to the data. Data is downloaded from the individual's App or Token only when an individual is tested positive for COVID-19, so that contract tracers can swiftly identify the close contacts of the affected individual.

As of 1 November 2020, there has been more than 2.5 million App downloads, and more than 570,000 Tokens have been collected.

13 To complement the technical and process measures, the Government has also enhanced its data security audit framework and implemented an enhanced third-party management framework. The audit framework was enhanced to cover end-to-end data security risks rather than only data in individual systems. It ensures that higher risk systems are inspected more frequently and focuses on the effectiveness of the safeguards besides mere compliance with policies. The enhanced third-party management framework guides agencies in ensuring that third parties protect Government data according to the high standards of data protection that the Government places on itself. The framework helps agencies to assess the risks when engaging a third party for a project, stipulates the necessary standards and governance needed throughout the project lifecycle, and establishes an audit regime to verify that the third party is compliant with stated policies. Industry players have reflected that the framework has helped them to better understand the Government's expectations of their non-Government partners.

Outcome 2: Detect and Respond Swiftly to Data Incidents

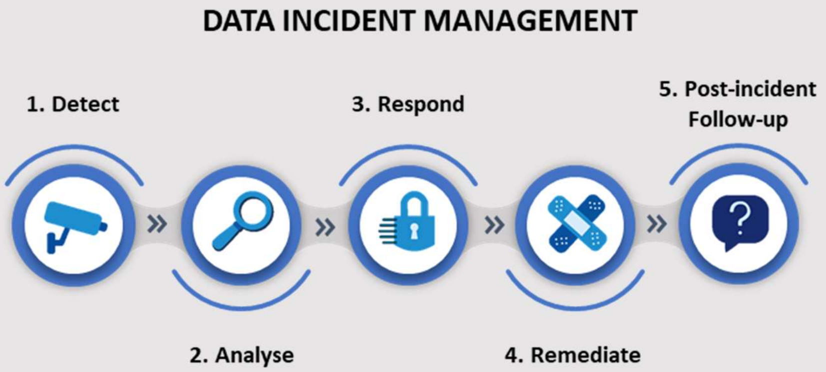
14 It is not possible to completely eliminate the risk of data incidents. We must therefore remain vigilant and be well-prepared to detect data incidents quickly and respond effectively to manage the impact of the incidents.

15 In 2020, we established the Government Data Security Contact Centre (GDSCC) for members of the public to report data incidents involving government data or government agencies. This is part of our efforts to encourage members of the public to work with the Government to strengthen the overall public sector data security regime. This enables the Government to better detect data incidents and take remediation actions if necessary. Such reports from the public augment our existing channels for detecting data incidents, such as active monitoring of log files and network traffic to identify anomalous activity.

16 For a more coordinated and effective response to data incidents across the Government, we also enhanced the public sector Data Incident Management Framework (see Box 4). All public agencies are required to carry out cyber and data security incident exercises annually, to ensure that they are able to implement the processes in this framework and prepared to respond swiftly and decisively to data incidents.

Box 4: Enhanced Data Incident Management Framework

Our Enhanced Data Incident Management Framework is structured around the five stages for managing incidents:



We have reviewed and improved the processes for each stage, such as introducing:

a. A standardised process to notify individuals affected by data incidents, which could cause them significant harm. This is in line with the PDPC's notification framework.

b. A standardised post-incident inquiry process that agencies must carry out in order to identify the root cause(s) of the incident and address it effectively.

Outcome 3: Competent public officers embodying a culture of excellence

17 Every public officer must play his/her role in safeguarding the data used. These must be undergirded by a culture of excellence towards using data securely. He/she will need to move beyond compliance with baseline requirements to being sensitive to data security risks and proactively managing them.

18 The Government has issued guidance to different groups of public officers – top leadership, key appointment holders, ICT and data teams, and general public officers – to clarify their roles and responsibilities in securing public sector data. We have also identified the relevant data security competencies needed for each group of officers to play their roles well. Structured training programmes have been rolled out to upskill public officers in data security, such as an e-learning module on data security for all public officers (see Box 5). We have also conducted seminars and disseminated regular newsletters to key appointment holders (Chief Information Officers, Chief Data Officers, Chief Information Security Officers) to apprise them of the latest data security trends and share best practices that they could adopt in their agencies.

Box 5: E-Learning Module for Public Officers

To raise officers' baseline competency in data security, an e-learning module on data security was officially rolled out to all public officers on 8 May 2020.

The revamped module focuses on how to effectively protect data to prevent data compromises, how to detect and respond to data incidents, and the impact and consequences of data security breaches. The module also includes a post-course declaration for officers to attest that they have understood their responsibilities and accountability when handling Government data.

All officers are required to complete the module and an accompanying quiz annually. Officers who are new to the public service have to complete the module and the quiz within 3 months of joining the service.

Outcome 4: Accountability for data protection at every level

19 All public agencies and public officers must uphold high standards to protect Government data. In 2020, we mandated that public sector agencies and Heads of Agencies are to manage data security and cybersecurity as organisational priorities. All Agency leaders are to treat data security and cybersecurity risks as key enterprise risks and institute key performance indicators to monitor the state of their organisations' data security and cybersecurity. Heads of Agency are also accountable for developing a strong culture of data security-consciousness within their agencies.

20 Besides public officers, third parties such as vendors and contractors often handle Government data on behalf of the Government. To ensure that they are held accountable when handling Government data, work is underway to amend the Personal Data Protection Act (PDPA) to cover agents of the Government within its scope and to bring non-public officers to task for recklessly or intentionally mishandling any personal data. The PDPA is expected to be amended by end-2020.

21 The Government is also committed to providing the public with more information about the Government's personal data protection policies and standards, and its data protection efforts. In 2020, we launched a new microsite, "A Secure Smart Nation" for the public to access information on the Government's approach to cybersecurity and data security (see Box 6).

Box 6: Secure Smart Nation Website

The Government has launched a microsite, "A Secure Smart Nation", (https://go.gov.sg/SecureSmartNation) for the public to find out more about the Government's cybersecurity and data security approach and the requirements imposed on public agencies. The Government's personal data protection policies and Third-Party Management policies have been published on the microsite. It also houses the platform for members of the public to report incidents involving government data or Government agencies to the GDSCC.

22 The Government has also stepped up its engagement of data protection professionals from the private sector to ensure that industry best practices on data protection are continually incorporated into our programmes (see Box 7).

Box 7: Engagement of Data Protection Professionals for TraceTogether Tokens

On 19 June 2020, experts from Singapore's tech community were invited to "tear down" the TraceTogether Token and provide feedback for improving the device. These experts included hardware hacker Dr Andrew Huang; firmware developer Mr Sean Cross; Mr Roland Turner, Chief Privacy Officer of TrustSphere; and Mr Harish Pillay, Chief Technology Architect at Red Hat.

The Government also engaged data privacy experts on 20 July 2020 to discuss the application of the Government's data governance and protection principles to the TraceTogether Tokens. These data protection professionals and experts gave feedback and suggestions on improving the governance of the data collected through the TraceTogether programme, including how these could be communicated to the public.

Outcome 5: Sustainable and resilient data security regime

23 Appropriate organisation and governance structures must be put in place to ensure that our data security regime keeps up with emerging threats and new technologies. In 2020, the Government established the Digital Government Executive Committee for Cyber and Data, chaired by Permanent Secretary of Smart Nation & Digital Government, as the high-level body to oversee public sector data security. The Government Data Security Unit was also set up to drive the implementation of the PSDSRC recommendations and engage agencies and officers on improving their data security practices. These initiatives ensure that there is sufficient focus and attention to continuously improve the Government's data security regime.

Effectiveness of Personal Data Protection Initiatives

Data Incidents in the Government for FY2018 to FY2019

24 There was a total of 75 data incidents reported in FY2019, up from 51 in FY2018. The number of data incidents reported in the first half of FY2020 is similar to that in the same period in FY2019.

No. of Data Incidents Reported			
Time taken to address data incident	**FY2018**	**FY2019**	**FY2020 (up to 30 Sep 2020)**
Within 48h of detection	50	75	37
Between 48h and 7 days	1	0	0
Total	51	75	37
Note: Time taken to address the incident is used as an indicator of the impact of the data incident – the longer the time taken, the larger the impact.			

25 From FY2018 to 2019, there has been a 50% increase in the total number of data incidents reported. This is in tandem with trends seen in the private sector and globally. The number of data incidents reported has increased due to an improved understanding among officers of what constitutes a data incident and heightened awareness to report all incidents, no matter how small, so that the rest of the Public Service can learn from them. This is a result of stronger engagement of public officers on data security matters. On the other hand, the number of data incidents which required extensive effort and time to address has dropped from 1 incident in FY2018 to 0 incidents in FY2019 and the first half of FY2020.

Lessons from the Data Incidents

26 The two main causes of data incidents in FY2018 to the first half of FY2020 were related to human error:

a. Oversight when handling data. For example, inadvertently emailing sensitive data to the wrong recipients, and misplacing IT equipment containing sensitive data; and

b. Failure to follow established processes to secure data. For example, to save time, the software developer did not adhere to the proper procedures and deployed software that contained bugs, which could have resulted in unintended exposure of sensitive data.

27 Technical measures had often been effective in mitigating the damage and impact of data incidents. The majority of the incidents reported were not assessed to have significant impact on the agency or individuals affected as protection measures had been in place to mitigate the impact. For example, the misplaced IT equipment were encrypted; the sensitive data contained therein would not be usable to unauthorised users who attempted to extract data from these devices.

28 In 2021, the Government will continue to invest in technical tools as the first line of defence against data compromises. This includes the Whole-of-Government Data Loss Prevention programme, which will be integrated into the ICT systems and user devices, and will be completed by end-2021.

29 More must also be done to tackle the root cause of human error. While the policies and processes on handling sensitive data are generally sound, many of the data incidents occurred because officers failed to follow these established procedures and protocols. The officers found responsible for these data incidents had been duly disciplined, with punitive measures ranging from counselling and formal reprimands, to financial penalties.

30 However, disciplinary actions are not sufficient. There is a need to develop a deeper appreciation of the importance of data security among public officers. The Government will therefore ramp up our efforts to increase data security awareness and knowledge amongst public officers in 2021. This includes embarking on more intensive campaigns to engage officers on data security and sharing lessons learnt from past data incidents in newsletters and at workshops, among other things. Starting in 2021, the Government will conduct regular ICT and Data incident management exercises for public agencies and public officers to practice and improve their incident management processes. These are first steps towards inculcating a culture of excellence in sharing and using data securely, which will require sustained efforts across many years at all levels of the organisation.

Emerging Trends

31 While the Government continues to enhance our data security regime against current threats, we must also respond to emerging trends and threats.

32 A growing area of interest is the use of biometric data and the attendant data protection and security concerns. Biometric data is increasingly being used as a convenient and secure form of identity verification for access to digital services and secure premises. For example, in September 2020, the Government announced that users of Singapore's National Digital Identity SingPass will be able to use biometric face verification services to transact seamlessly and securely with digital services from the public and private sectors.

33 Biometric data has unique characteristics that set it apart from other types of personal data. For example, biometric data is often immutable, that is, it cannot be easily replaced once compromised. The Government is working on additional guidelines, built on top of the Government's existing data protection requirements, to guide public agencies in using biometric data responsibly to discharge their functions while safeguarding the data well. The guidelines are expected to be completed by end-FY2020.

Conclusion

34 The Government has embarked on a journey to become digital to the core and drive Singapore to become a Smart Nation. The pace of digitalisation has accelerated with the advent of the COVID-19 pandemic. A recent survey reported that nearly 75% of Singapore firms are accelerating their digitalisation efforts due to COVID-19 (Straits Times, 10 Sep 2020). The public sector has also adapted accordingly. The Government uses data and digital tools extensively to aid our fight against COVID-19 and to continue serving citizens while minimising physical contact. However, such extensive storage, transfer and use of personal data and digital tools also increase the potential areas of attack that malicious actors can exploit.

35 Our increased digitalisation must therefore be accompanied by a strong and robust data security regime. The Government will continue to update our measures to ensure that our data security regime is resilient to these threats. We will press on with the implementation of the technical and process measures in the next few years, and re-architect the relevant systems. We will keep abreast of emerging technologies that can strengthen our data security regime and incorporate them into our systems where practical. And because we can never completely eliminate the data incidents, we will continue improving our processes so that we can respond effectively and rapidly to such events, and minimise the impact on our citizens. Public officers must also remain vigilant and aware of these threats, and the Government will continue to build a culture of excellence for all public officers to use data securely. This will put us in a better position to use data well to better serve the public.