**SMART NATION & DIGITAL GOVERNMENT OFFICE**

# ANNUAL UPDATE ON THE GOVERNMENT'S PERSONAL DATA PROTECTION EFFORTS

Nov 2020

## Highlights of the Government's Initiatives

In 2020, the Government focused its data security efforts on implementing the recommendations made by the Public Sector Data Security Review Committee (PSDSRC) in Nov 2019. Examples of initiatives leading to each outcome include:

**Outcome 1:**
**Protect Data and Prevent Data Compromises**

- Implemented technical tools and change in work processes.
- Implemented the enhanced audit framework.
- Implemented third-party management framework.

**Outcome 2:**
**Detect and Respond Swiftly to Data Incidents**

- Established Government Data Security Contact Centre (GDSCC) for public to report incidents.
- Enhanced the public sector Data Incident Management Framework.

**Outcome 3:**
**Competent Public Officers embodying Culture of Excellence**

- Issued guidance to clarify roles and responsibilities of different groups.
- Set up E-learning module on data security for all public officers to complete annually.

**Outcome 4:**
**Accountability for Data Protection at every level**

- Mandated leadership to manage data security as a key organisational priority.
- Amended PDPA to cover agents of Government and non-public-officers.
- Launched "A Secure Smart Nation" microsite; published Government's personal darta protection policies.

**Outcome 5:**
**Sustainable and Resilient Data Security Regime**

- Established Digital Government ExCo for Cyber and Data.
- Set up Government Data Security Unit to drive implementation of recommendations.

## Improvements Made

- ✅ Improved audit and third party management processes
- ✅ Enhanced data incident management processes
- ✅ Strengthened accountability measures
- ✅ Instituted a clear and structured approach to improving competencies and culture
- ✅ Strengthened data security organisational structures
- ✅ Improved transparency of public sector data security regime

## Effectiveness of the Government's Initiatives

### No. of Government Data Incidents Reported

| | |
|---|---|
| FY2018 | 51 |
| FY2019 | 75 |
| FY2020 (Up to 30 Sep) | 37 |

> All data incidents reported in FY2019 and FY2020 were **addressed within 48h of detection**

The 50% increase in total number of data incidents reported from FY2018 to FY2019 is in tandem with trends in the private sector and globally. The number of incidents reported has increased due to an **improved understanding among officers** of what constitutes a data incident, and **heightened awareness of the need to report all incidents**, no matter how small. At the same time, the number of incidents reported that required extensive resources and time to address (as a proxy of scale/impact) fell from 1 in FY2018 to 0 in FY2019 and FY2020 (up to 30 Sep).

## Lessons Learnt from Data Incidents

**1** **Technical measures were effective in mitigating the impact of incidents**. Most FY2019 data incidents reported were not "major" as damage were mitigated by technical safeguards.

**2** **Main cause of incidents is public officer's oversight** when handling data and failure to follow established processes to safeguard data. The Government will ramp up efforts to build a culture of excellence towards using data securely across public service.

**3** **Risk of data incidents cannot be fully eliminated**. The Government will be conducting regular ICT and data incident management exercises from 2021 to ensure that agencies are ready to respond swiftly to incidents and take effective remediation actions.

The full annual update on the Government's personal data protection efforts for 2020 can be found at **go.gov.sg/SecureSmartNation.**