ADEPT ACADEMY

FUNDAMENTALS OF THE PERSONAL DATA PROTECTION ACT (2020)

23 Hours (3 Days Course)
Suitable for Executives, Supervisors, Managers and Management Team

COURSE OBJECTIVES

To equip DPOs with basic knowledge and skills in complying with the PDPA

Obtain consent to collect, use or disclose individuals' personal data

Cease retention or anonymize personal data when it is no longer necessary for business or legal purposes

	Full Course Fee (w/gst)	21-39 years old after 50% funding	> 40 years old after 70% funding*
Non-Singaporean	$700 ($749)	$700 ($749)	$700 ($749)
Individual / SME / Non SME	$700 ($749)	$350 ($399)	$210 ($259)

Prices in () include 7% GST
* After 70% funding for SME-sponsored Singaporeans and PRs under Enhanced Training Support for SMEs (ETSS) scheme

Damien Tay

☎ (+65) 8587 6692

✉ damien.tay@adeptacademy.com

2 Kallang Avenue, #03-08
CT Hub, Singapore 339407

ELITEZ
DATA PROTECTION

Data Breaches – Not If, But When

Since 2015, more than **28,600** complaints have been made against various organizations in Singapore to the PDPC

Having a **Data Protection Management Program** in place not only enables an organisation to respond swiftly in managing any data breaches, it also establishes a robust data protection infrastructure. This provides confidence to stakeholders and fosters high trust relationships with customers and business partners.

Organisations can build up basic data protection capabilities and achieve compliance with the PDPA through the Data Protection Management Programme offered by Elitez Data Protection. It comprises of:

1. **one-time setup service (inclusive of a 6-month review)** covering the scope below; and
2. **a 1-year annual retainer service (commences after completion of one-time setup service)** consisting of bi-annual review and refresher on policies, incident management and data protection practices.

One-Time Setup Service

Data Protection Management

1. Assisting with the appointment and registration of a Data Protection Officer with ACRA
2. Identify risks and gaps using PDPA Assessment Tool for Organisations (PATO)
3. Document data assets and flows using a Data Inventory Map (DIM)
4. Establish physical, technical and administrative measures for data protection
5. Establish a process for handling access and correction requests
6. Develop a Personal Data Protection and Security Policy (PDPSP) for internal stakeholders
7. Develop Personal Data Privacy Notices (PDPN) for external parties
8. Establish a complaint handling procedure regarding personal data issues

Data Breach Management

1. Establish a data breach management team composition;
2. Develop a complaint handling procedure; and
3. Develop a breach incident response plan using the C.A.R.E model

Staff Training Management

1. Developing a staff training and communications plan for all employees
2. Facilitating all staff to complete the PDPA e-learning programme
3. Assisting with the identification of key personnel and facilitating the attendance of these key personnel at the following courses:
    a. Fundamentals of Personal Data Protection Act; and
    b. Practitioner Certificate in Personal Data Protection.

6-Month Review (complimentary)

1. Carry out review and update of:
    a. Data protection policies
    b. Data breach response plan
2. Refresher on data protection awareness training for key employees on handling personal data
3. Conduct phishing simulation exercises to train the employees to be alert
4. Conduct table-top exercise to test data breach response plan

Safeguarding Your Business & Data

Contact us at **DPO@elitez.asia** to find out more today!

2 Kallang Avenue CT Hub #03-08 Singapore 338407
www.dataprotection.elitez.asia +65 6602 8282

Ministry of Communications and Information

04 Mar 22

Speech by Mrs Josephine Teo, Minister of Communications and Information, at the Ministry of Communications and Information Committee of Supply Debate on 4 March 2022

☰ Listen ▶

Category: Public Comms, Personal Data, Libraries, Infocomm Media, Government Technology, Digital Readiness, Digital Defence, Cyber Security, Others

Type: Speeches, Parliament QAs

Introduction

1. Mr Chairman, I thank Members for their questions and interest.

Digital is shaping the way we live, learn, work, and play

2. Earlier in the COS debate, I updated members about the progress of our Smart Nation initiative. Digital technologies are very much a part of our daily lives. They have brought day-to-day conveniences, new and improved jobs for our people, and growth opportunities for our businesses.

3. But a digital future can be daunting as well. Enterprises struggle to get the right technologies and talents. Workers worry about being replaced. Seniors may feel left out. Parents are concerned about the impact on their children.

4. MCI understands all these concerns. Our mission is to ensure our people can reap the benefits and rewards of technology, while safeguarding our safety and security. Our vision of Singapore's digital future is one that is economically vibrant, socially stable and cyber secure.

5. MCI's theme for this year's COS is "Building a Vibrant and Secure Digital Future Together". The economic opportunities of the digital domain have brought about tremendous transformation and growth in Singapore. Since 2016, the Information and Communications Sector has grown by an average of 9.4%, well above the GDP growth rate. Across the economy, the number of ICT professionals has risen from around 180,000 in 2016 to 216,000 in 2020. The positive impact on the wider economy is evident. SMS Dr Janil and MOS Kiat How will say more about these later. This dynamism is equally evident in our society. Parl Sec Rahayu will provide an update on our efforts to promote digital empowerment and wellness. To harness the full potential of the digital domain, I will focus on two aspects of growing importance. First, how we will enhance regulations in the digital domain to better protect ourselves and our loved ones, and to strengthen digital security and resilience. Second, how we will sustain and deepen engagement of every Singaporean in the digital era, to preserve and enhance social cohesion.

Governing and securing our digital spaces

6. According to surveys carried out by MCI, 76% of Singaporeans said they feel comfortable using digital technologies, but only 40% have installed cybersecurity apps on their mobile phones. Among seniors aged 60 and above, 67% use instant messaging, and over half search for information online. But only 40% could recognise and avoid phishing attempts.

7. Clearly, using technology alone is not enough, it's only half the story. We also need to better protect ourselves and our loved ones from its risks and threats.

8. MCI has three priorities to Govern and Secure Our Digital Spaces.

Protecting our People in Online Spaces

9. The first is to better protect Singaporeans from harmful online content, especially the young and vulnerable. A recent Straits Times survey found that among children aged seven to nine, two-thirds use a smartphone daily, yet a third of parents do not know who their children interact with on social media. Last year, a National Youth Council poll found that two-thirds of youths had experienced online harms such as harassment and unwanted advances. Many developed distrust towards others, and experienced stress and anxiety. Last year, a 10-year-old Italian girl lost her life while participating in an online "hanging challenge". Users were encouraged to choke themselves until they pass out, while livestreaming on TikTok.

10. Harm can be caused not only to children. In 2019, social media companies struggled to remove re-shares of the video showing a gunman firing on Muslims in a New Zealand mosque. In 2021, rioters who stormed Capitol Hill in the US used social media to organise and amplify their messages.

11. Governments worldwide have responded to online harms with new laws. In 2017, Germany enacted its Network Enforcement Act, which requires platforms to act on unlawful content reported by users. Last July, Australia enacted an Online Safety Act, which introduces basic safety expectations for online service providers. The UK's draft Online Safety Bill will create a duty of care for online platforms towards their users, including requirements to take action against harmful content.

12. Dr Shahira Abdullah, Ms Tin Pei Ling, Dr Wan Rizal and Mr Don Wee are right to ask what more can be done in Singapore.

13. Some measures are already in place. Internet Content Providers must comply with the Internet Code of Practice. IMDA has powers to take down content that goes against "public interest, public morality, public order and national harmony". IMDA can also direct Internet Service Providers to block access to prohibited websites. To manage children's access to websites and online services, IMDA requires Internet Service Providers to offer filtering services for parents to subscribe to. To reduce exposure to age-inappropriate entertainment content, Over-The-Top and Video-on-Demand streaming services with content rated NC16 or higher must provide parental controls.

14. In a 2020 study of online safety for children in 30 countries, international think-tank DQ Institute ranked Singapore fourth. This gives us some comfort. But with the growing risks of online harms, we must step up efforts to keep online spaces safe, especially for our children.

15. Online platforms accessible by users in Singapore can and must take greater responsibility for user safety. They should endeavour to keep online spaces free from harmful content, including age-inappropriate content, such as violent and graphic content, and content that promotes sexual violence.

16. To raise the baseline standard for online safety, we plan to introduce Codes of Practices in three new areas.

17. The **first area is child safety**. It will require platforms to have robust systems in place to minimise exposure of children and young persons to harmful content. These include content filters for child accounts, and mechanisms for parents to supervise and guide their children online.

18. The **second area is user reporting**. Last year, MCI formed the Sunlight Alliance for Action to tackle online harms. Members of the Alliance want internet platforms to be diligent in assessing flagged content, and remove harmful content without delay. But many social media platforms tell us that they cannot be fully aware of all the content that needs moderation. Much of it is user-generated and the quantity, voluminous. User reporting is therefore an important way to close the awareness gap and promote prompt follow-up action. It will require platforms to set up easy-to-access mechanisms for users to report harmful content, to be responsive in evaluating and acting on these reports, and to apprise their users in a timely manner of the actions taken. This will empower users to highlight harmful content they come across and prevent further spread.

19. The **third area is platform accountability**. It will require platforms to provide information on what they are doing to keep users safe. This includes the prevalence of harmful online content on their platforms, the user reports they have received and acted upon, and the systems and processes they have in place to address harmful online content. Users can then compare the approaches taken by platforms and make informed decisions about which to engage or disengage.

20. Similar to existing Codes of Practice administered by IMDA, these new Codes will have the force of law. They will require relevant online platforms to take more actions to create a safer online environment. We will study how the Codes can be effectively enforced, including through appropriate legislative updates.

21. We are also working with the Ministry of Home Affairs to provide Singaporeans with more protection from illegal activities carried out

online. This includes strengthening our levers to tackle online scams, as well as a broader suite of criminal activities taking place online, such as child pornography, terrorism, and content that incite violence.

22. MCI has frequent engagements with our international and industry partners on issues relating to user safety. We will continue to consult extensively as we develop these new Codes.

23. But the evolving nature of the digital domain will always test the way we design our regulations, as pointed out by Ms Tin. We need to be clear and unambiguous to uphold security and trust, while not being overly prescriptive or stifling innovation. The scope of coverage must be wide enough without being excessively expansive. Simplicity must not be achieved at the expense of effectiveness.

24. In many ways, our regulatory approach for the digital domain will be similar to how technology services are launched these days, as Minimum Viable Products that will be improved iteratively. Put another way, perfect must not become the enemy of good. Instead, we must be prepared to regularly update these Codes, introduce new ones or streamline outdated ones, to deal with emerging issues and new technologies. Only by doing so can we harness the rich potential of exciting new technologies while guarding against their attendant risks.

Strengthening our Cybersecurity

25. Mr Chairman, another important priority of MCI is to strengthen our cybersecurity. Mr Shawn Huang, Ms Hany Soh, and Mr Xie Yao Quan asked what more we are doing to guard against cyber threats.

26. Since 2018, the Cybersecurity Act has provided a legal framework for CSA to oversee and maintain our national cybersecurity. The Act is currently focused on securing and protecting our Critical Information Infrastructure. These computer systems deliver essential services in the physical world, such as water and power.

27. Given the unfolding situation in Ukraine, we must be alive to the heightened risks. Singapore is gravely concerned over the cyberattacks against Ukraine's government websites and national banks. It illustrates how essential services can be disrupted remotely and quite easily. Singapore may be geographically distant from the theatre of action. But we cannot disregard the potential knock-on effects arriving on our shores. This is why, earlier this week, we advised local organisations to beef up their cybersecurity posture.

28. But even before the current situation in Ukraine, cyber threats have become more prevalent. Between 2020 and 2021, Singapore observed a 73% increase in reported data breach and ransomware incidents. As our digital realm expands, so too the threat surface.

29. The scale and impact of such attacks elsewhere have also become more serious. Attacks on systems that run physical infrastructure such as energy grids and fuel pipelines have real, tangible impact. The ransomware attack on US Colonial Pipeline last year, for example, caused fuel shortages across the US East Coast.

30. CSA has been reviewing the Cybersecurity Act. To strengthen our defences, we need to address three key questions.

31. **First, how do we raise our situational awareness over Singapore's cyberspace?** Attackers are constantly on the lookout for serious vulnerabilities, like burglars looking for faulty locks and open windows. CSA must in some way do the same, but for a very different reason – so that we can advise people to fix their faulty locks and close their windows quickly. In cyberspace, this means to patch known software vulnerabilities, before malicious actors compromise our systems and steal our data.

32. **Second, what should be considered as Critical Information Infrastructure, or CII?** The Act currently recognises physical networks and systems as CII. With the shift to virtualisation, we must be able to recognise virtual assets as CII too, such as systems hosted on the cloud. We need to ensure these virtual assets are properly protected too, including those that may not be hosted in Singapore.

33. **Third, how do we secure important digital infrastructure and services beyond CIIs?** Digital infrastructure and services are the backbone of our connectivity, computing and data storage needs. If disrupted or compromised, there could be serious knock-on effects. Imagine the chaos of not having access to emails, websites, and apps. We will consider how to apply a risk-based approach to protect these infrastructure and services, and for them to recover quickly when attacked.

34. We intend to complete this review by 2023, factoring in stakeholder and public consultations. The Act will be updated thereafter.

Strengthening Safeguards for Consumers and Businesses

35. Mr Chairman, Mr Sharael Taha asked how we could enable businesses to innovate and grow, while safeguarding consumers and their personal data. This is also a priority.

36. Data is a critical resource in the digital economy. In 2012, we enacted the Personal Data Protection Act, or PDPA. It strikes a careful balance between allowing organisations to harness data for innovation and growth, and ensuring proper safeguards and accountability. In 2020, to adapt to the evolving digital landscape, we amended the PDPA. Among several amendments, we explicitly recognised business improvement as a legitimate use of data.

37. Early results from ongoing surveys are encouraging. Close to 90% of businesses agreed that the PDPA helps them prepare for the digital economy. More than 80% of consumers said the PDPA helped them trust that their personal data is protected from misuse by organisations.

38. To uphold this trust, organisations must continue to take ownership and be held accountable, especially those that hold sizeable volumes of personal data. This is why the PDPA amendments in 2020 raised the maximum financial penalty for data breaches to $1 million, or 10% of local annual turnover for organisations whose turnover exceeds $10 million, whichever is higher.

39. As a result of the pandemic-induced economic uncertainty, the implementation of the new penalties was temporarily held back. With sufficient lead-time given to businesses, the penalties will now take effect from **1 October 2022**.

40. We will also strengthen safeguards in other areas. Currently, consumers and small businesses try to resolve contractual disputes with their telco or media service providers directly, or through existing dispute resolution options. These can be costly and less consumer-friendly. To supplement these options, IMDA will launch an **Alternative Dispute Resolution Scheme** which is designed to be affordable and effective. When a case is brought to the ADR, it will be mandatory for the service providers to participate in the resolution process. From April, this will provide a new helpful channel to resolve such disputes.

41. Mr Chairman, the three priorities I have described to Govern and Secure Our Digital Spaces will form the building blocks of a vibrant and secure digital future.

Engaging Singaporeans in a Digital World

42. Sir, technology has changed the way we interact; with each other, our communities, and the world.

43. The global media and information landscape has become more diffused, with competing narratives and echo chambers, and more news sources than anyone can keep up with.

44. Mr Don Wee rightly pointed out the need for trusted information sources and genuine engagement, and a holistic approach to target the spread of misinformation.

Government Communications

45. Indeed, these have been critical in combating the Covid-19 pandemic. We could not have handled a public health crisis if the public didn't trust the health authorities or didn't believe the information they were receiving. That is precisely why, from the very outset, we resolved to keep the public informed as fully and as expeditiously as possible. We were determined to tell it as it is, never fudge or sugar-coat, never hide. As the Prime Minister observed recently, if we had been a low-trust society, people would not have understood the need for safe management measures, or abided by them. Our infection rates would be higher, far fewer people would be vaccinated, and many more people would have died. To preserve this trust, we must also have appropriate laws. For example, POFMA allowed us to take swift action on 20 occasions to curb COVID-19-related misinformation, and prevent falsehoods from taking root.

46. The COVID-19 pandemic has therefore underlined the crucial importance of retaining public trust and maintaining trusted sources of information.

47. MCI has done this by expanding and refreshing our communications channels and launching targeted campaigns, like VacciNationSG to support our vaccination drive. Gov.sg's 10 platforms have close to 2 million more subscribers compared to before the pandemic. We commissioned e-Getai shows for seniors that received over 7.5 million views, and catchy music videos with over 9 million views online.

48. To better engage Singaporeans from all walks-of-life and understand their concerns, REACH expanded its digital outreach through e-Listening Points and virtual dialogues. In 2021, more than 70,000 Singaporeans contributed feedback to REACH, up from 59,000 in 2020.

49. Through these concerted efforts, polls show that 3 in 4 members of the public think that the Government has provided sufficient information on COVID-19 in recent months. Over 86% agreed that these messages helped in their decision to get vaccinated.

50. It is critical that we maintain these high levels of trust, as we strive to bounce back from the COVID-19 pandemic, and see through future crises as Singapore Together.

Public Service Media

51. Our local media companies play an important role in this mission to inform and engage our citizens. They help to keep Singaporeans united, by providing a Singapore lens through which citizens can make sense of global events; presenting an authoritative source of information that cuts through the noise of an online space chock-full of clickbait content and misinformation; and producing content in our official languages that celebrates our diverse culture and creates shared experiences for all Singaporeans.

52. Clearly, our local media companies serve a broader mission beyond commercial success.

53. This is why the Government put our support behind SPH Media Trust. We have explained the background extensively during the Parliament Sittings in May 2021 and February 2022, but I will reiterate two key points. First, our local media, like media outlets across the world, have seen their advertising and subscription revenue drastically reduced, buffeted by the rise of digital content platforms and new avenues for free content. Second, while our local media enjoys good reach – today, Mediacorp and SPH Media reach 96% of Singaporeans – there are no easy answers on how they monetise this reach. We hope they can become self-sustaining, but it remains to be seen whether or when this can happen.

54. Mr Leong Mun Wai said SPH is Government owned. That is incorrect. If it was, there would be no question today of public funding. He then asked if the SPH listed company could be made to contribute more to the new SPH Media Trust. The shareholders voted and agreed to an initial injection of $80 million cash and $30 million worth of shares for SPH Media Trust. If the restructuring proposal involved an even higher contribution, the shareholders could have walked away. The CLG might not have been formed, and the SPH media business could have remained on its trajectory of decline, with scant hope for revival. In time to come, there would be nothing worthwhile to preserve.

55. Parliament has been fully briefed on the need for the restructuring and accepted that our local mainstream media is worthy of public funding. When compared to the investments seen elsewhere in the world, the amount of funding to support our local media's transformation must be meaningful in order for their efforts to have a chance to succeed. We cannot be half-hearted about it. I have also explained in detail how the Government will keep them accountable.

56. Let us now direct our attention on charting the way forward, such as those highlighted by Ms Hany Soh on how the media can better meet the needs of different demographics. For example, Mediacorp is working with their news broadcasters, as well as clan associations, to identify new talent to sustain dialect radio news broadcasts. Mediacorp produces an animation series on sustainability and environmental awareness, so that parents and their children know why this is important, and how they can contribute to this national priority. Left to the free market, such programmes are unlikely to be viable.

57. I therefore urge Members to give our local media and journalists the fullest support because they deserve it.

Media Industry

58. As the media industry adapts to the rise of digital, exciting new opportunities have also emerged. The global market for content is set to grow to more than 500 billion Singapore dollars by 2025, half of which is in the Asia-Pacific.

59. Singapore is well-positioned to benefit, because of our robust intellectual property and legal frameworks, and our role as a connector between markets and cultures.

60. Global names like Walt Disney, iQIYI, WarnerMedia, and Netflix already have a presence here, alongside homegrown players like Beach House Pictures, one of Asia's largest independent production companies.

61. We will continue to support these companies and our talents by exploring new partnerships with creator networks like Titan Digital Media, platforms like YouTube, TikTok, and Twitch, and online creators, and partnering industry to improve content quality and better understand viewer preferences through data, AI and virtual production.

62. These efforts will position us as a hub for content that is both "Made **in** Singapore" and 'Made **with** Singapore".

63. Mr Chairman in Mandarin please:

打造安全璀璨的数码未来

64. 对许多国人来说，网络服务就如水电一般，是生活中的必需品。

65. 在现今世界里，打造一个蓬勃安全的数码未来，甚至攸关一个国家的生死存亡，繁荣发展。

66. 我国将继续面对未知的挑战，但我们不会放弃。

67. 新加坡政府将通过各项措施致力于帮助每一名国人，在数码时代，取得成功。

68. 处于各个数码阶段的中小企业，都有机会在数码旅程中跨进一步。即使面对种种压力，也能闯出新天地。

69. 处于各个领域的工友将能精深技能。大家都会得到帮助，提升数码技能，改善生计。

70. 年长者将有机会活到老，学到老，掌握科技，保持社会联系。

71. 孩童将受到更好的保护，不轻易受到不良内容，不法之徒的侵害。

72. 我们也正努力巩固数码设施的安全，以增强国人、企业对数码未来的信心。

73. 在政府、业界和国人的共同努力下，我有信心，新加坡将能打造出一个安全、璀璨的数码未来。我们深爱的小红点，在数码未来里，也将继续在国际舞台上发光发亮！

Conclusion

74. Mr Chairman, I have outlined MCI's priorities to Govern and Secure our Digital Space, and to Engage Singaporeans in a Digitalised World.

75. These are critical building blocks for Singapore's continued survival and success.

76. We look forward to partnering all Singaporeans to Build a Vibrant and Secure Digital Future Together!

PDF version of the speech
PDF

RELATED

04 Mar 2022
Building a Vibrant and Secure Digital Future, Together

06 May 2019
MCI's response to PQ on customer service by telcos

Our Agencies

CSA SINGAPORE

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

NLB

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Ministry of Communications and Information

Who We Are

About Us

Agencies

MCI Portfolios

Cyber Security

Digital Defence

Digital Readiness

Infocomm Media

Libraries

Personal Data

Public Comms

Careers and Grants

Careers

Job Vacancies

Scholarship

Grants

Public Consultation

Open Consultation

Archive

Media Centre

Pressroom

Stories

Parliament

Live-stream

Reporting in SG

Setting Up Shop

Working in Singapore

Get Accredited

Get Help

Useful Information

Contact Info

Feedback

FAQ