

## Editor's Note:

We're excited to unveil our new monthly CETA Buzz newsletter! Read on to find out what's hot here at CETA and subscribe to be alerted of our newest courses, events and collaborations across different industries! In the meantime, stay safe and keep well.

## PROTECT YOUR COMPANY'S INFORMATION AMIDST A RISE IN DATA BREACHES IN SINGAPORE



As our data is increasingly being collated, stored and distributed by third-party organisations we're becoming more vulnerable to data breaches which occur when there is unauthorized access to an organization's database of customer information. These may be caused by hacking, poor database security, the loss or stealing of physical equipment and even the accidental publishing of private data.

In June 2021, the Straits Times reported that several companies were fined for breaches and lapses that affected the personal data of more than 600,000 people - including their financial information. Established organisations, large and small, are not immune to the onslaught of personal data breaches, with the Personal Data Protection Commission (PDPC) meting out directives and penalties to those who have not kept up with measures to safeguard their data. Read more on this [here](#).

Continued vigilance is needed to prevent your data from being mishandled. This can be achieved through the implementation of good data security protocols - such as only allowing authorised access to sensitive information and instilling the following of best practices in the reading and disposal of data. If you are in charge of your organisation's data protection, it is imperative to arm yourself with knowledge of Singapore's Data Protection Act in order to build good defence systems that will keep your information safe and maintain credibility with your clients.

### Singapore's Data Protection Act: What you need to know

Singapore's Personal Data Protection Act (PDPA) was legislated in 2012, providing baseline measures needed for the protection of personal data in Singapore. It details various requirements governing the collection, use, disclosure and care of personal data in order to ensure that they are protected and used for legitimate purposes.

With PDPA regulations, the appointment of Data Protection Officers (DPOs) in each organisation is mandatory, and the penalty of data breaches has been increased to a maximum of 10 per cent of an organisation's annual turnover or \$1 million, whichever is higher.

With the increase in data breaches, the role of the DPO has also increased in importance. Our data protection courses provide you with in-depth information on the advisory guidelines and amended provisions of the PDPA 2020 and train you in identifying and assessing organisational policies with regards to these guidelines:

## SIGN UP TO GAIN ESSENTIAL KNOWLEDGE ON DATA PROTECTION

### Fundamentals of the Personal Data Protection Act (2020)

A 3-day curriculum that equips you with the necessary knowledge and skills required to facilitate compliance with the legislative and regulatory requirements of PDPA 2020. Click [here](#) for more info.

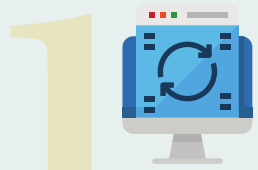
### Practitioner Certificate in Personal Data Protection (2020)

This 3-day preparatory course was developed for Data Protection Officers (DPOs) to equip them with practical data governance and data protection knowledge and skills. Click [here](#) for more info.



Follow these 3 tips to take the first step towards ensuring that your organisation complies to the provisions of the PDPA:

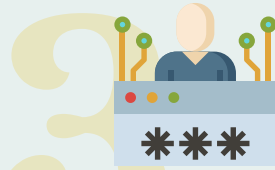
### 3 Ways To Prevent Data Breaches



Regularly update the patches for cyber security systems



Invest in the right security solutions for your data protection needs



Provide training sessions on updated security policies and procedures

Source: <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/data-breaches-on-the-rise-in-singapore-is-your-company-at-risk/>