

PDPO Compliance

PDPO Compliance in Hong Kong



The Personal Data (Privacy) Ordinance (PDPO) is Hong Kong's primary law governing the collection, use, and disclosure of personal data. It applies to both private and public sector organizations.

Key Provisions of the PDPO

- **Data Collection:** Personal data must be obtained fairly and lawfully, and for a specified and lawful purpose.
- **Data Accuracy:** Data must be accurate and kept up-to-date.
- **Data Retention:** Data should not be retained for longer than necessary.
- **Data Security:** Organizations must take appropriate security measures to protect personal data.
- **Data Subject Rights:** Individuals have the right to access, correct, and request deletion of their personal data.
- **Data Transfers:** There are restrictions on transferring personal data outside Hong Kong.

Recent Amendments to the PDPO

In 2012 and 2021, the PDPO underwent significant amendments to address evolving data protection challenges. Key changes include:

- Expanded definition of personal data: To cover more types of information.
- Increased enforcement powers: For the Privacy Commissioner for Personal Data.
- New data breach notification requirements: Organizations must notify the Privacy Commissioner and affected individuals of data breaches in certain circumstances.
- Clarifications on data subject rights: To enhance individuals' control over their personal data.

Challenges of PDPO Compliance

Similar to other jurisdictions, organizations in Hong Kong face challenges in complying with the PDPO, including:

- Defining personal data: Determining what constitutes personal data can be complex.
- Balancing privacy with business needs: Striking a balance between protecting data and achieving business objectives.
- Keeping up with technological advancements: Adapting to new technologies and their impact on data protection.
- Managing data breaches: Developing effective incident response plans.

Tips for PDPO Compliance

- Conduct a data audit: Identify and assess the personal data you hold.
- Implement data protection policies and procedures: Develop clear guidelines for data handling.
- Train employees: Raise awareness of data protection obligations.
- Conduct regular risk assessments: Identify and mitigate potential data protection risks.
- Stay updated on regulatory changes: Keep abreast of PDPO developments.

Learn more about [PDPO Compliance](#).



What's Next?

- ✓ Learn more about [ImmuniWeb Compliance Services](#).
- ✓ Read ImmuniWeb [Cyber Law and Cybercrime Investigation Blog](#).
- ✓ Join ImmuniWeb at the upcoming [Webinars](#) and [Events](#).
- ✓ Follow ImmuniWeb on [LinkedIn](#), [X \(Twitter\)](#), and [Telegram](#).
- ✓ Subscribe to ImmuniWeb [Newsletter](#).
- ✓ Try ImmuniWeb [Community Edition](#) Free Security Tests.
- ✓ See the benefits of ImmuniWeb [Partner Program](#).



The award-winning ImmuniWeb® AI Platform helps over 1,000 customers from over 50 countries to test, secure and protect their web and mobile applications, cloud and network infrastructure, to prevent supply chain attacks and data breaches, and to comply with regulatory requirements.



[API Penetration Testing](#)



[Continuous Automated Red Teaming](#)



[Dark Web Monitoring](#)



[Phishing Websites Takedown](#)



[API Security Scanning](#)



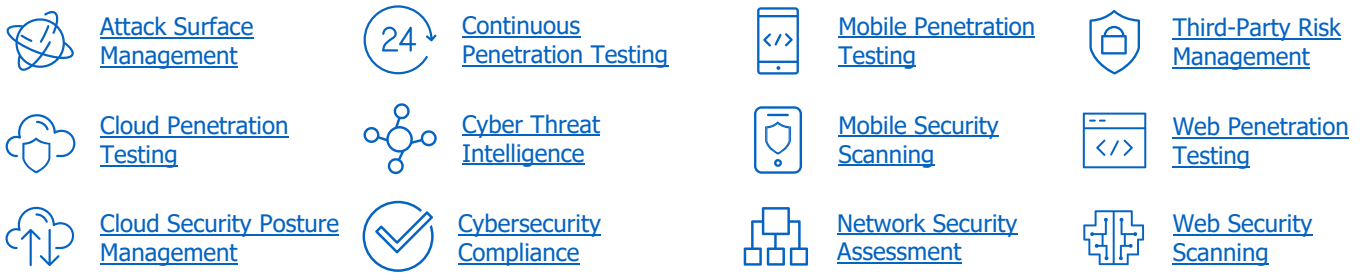
[Continuous Breach and Attack Simulation](#)



[Digital Brand Protection](#)



[Red Teaming Exercise](#)



One Platform. All Needs.
www.immuniweb.com

.....
This document is provided "as is" without any warranty of any kind for informational purposes only.