

2017内地—香港网络安全论坛

主题：促进数据安全有序流动，推动两地经济社会发展

2017年10月15日，厦门

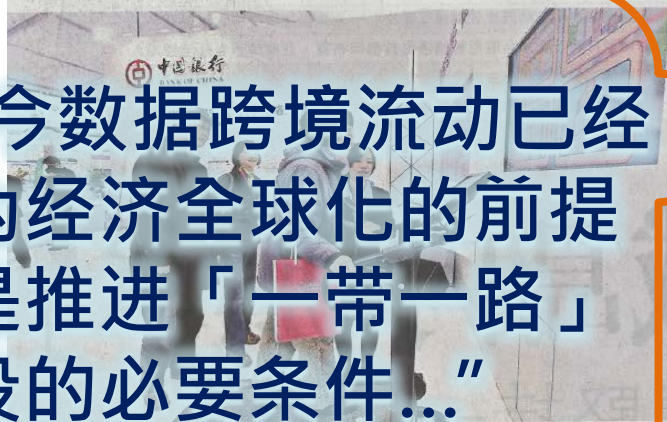
香港数据安全保护政策法律

保障 · 尊重個人資料
Protect, Respect Personal Data

黄继儿 大律师
香港个人资料私隐专员

網安法實施 強化個人信息保護

“当今数据跨境流动已经成为经济全球化的前提，是推进「一带一路」建设的必要条件...”



6月1日，《中華人民共和國網絡安全法》將正式實施，明確關鍵信息基礎設施保護制度。圖為網絡安全公眾體驗展

【大公報訊】6月1日，《中華人民共和國網絡安全法》（下稱網安法）將正式實施。日前，中國國家互聯網信息辦公室網絡安全協調局負責人就相關問題接受媒體採訪時表示，網安法明確了關鍵信息基礎設施保護制度，不是要限制數據依法有序自由流動。網安法的公布和施行，可加強對公民個人信息的保護，從法律上保障了廣大人民群眾在網絡空間的利益，維護國家網絡空間主權和安全。

綜合中新社、新華社報道：作為中國網絡安全領域的基礎性法律，網絡安全法在網絡安全領域具有里程碑意義，自去年11月7日經十二屆全國人大常委會第二十四次會議表決通過後，就一直備受各界關注。

近日，有外國協會和機構建議推遲實施網絡安全法，針對網絡安全法第35條規定的「關鍵信息基礎設施的運營者採購網絡產品和服務，可能影響國家安全的，應當通過國家網信部門會同國務院有關部門組織的國家安全審查」，擔心網絡安全法會製造貿易壁壘，限制國外企業和技術產品進入中國市場。

對此，這位負責人回應稱：「安全審查不針對特定國家和地區，沒有

國別差異，審查不會歧視國外技術和產品，不會限制國外產品進入中國市場。」他強調，網絡安全法明確了關鍵信息基礎設施保護制度，目的是要確保涉及國家安全、國計民生、公共利益的系統和設施的安全。

販賣50個人信息可入罪

網絡安全法規定關鍵信息基礎設施運營者在中華人民共和國境內收集產生的個人信息和重要數據應當在境內存儲。「這是對關鍵信息基礎設施運營者提出的要求，而不是對所有網絡運營者的要求。」這位負責人說，「不是所有的數據，只限於個人信息和重要數據，這裏的重要數據是對國家而言，而不是針對企業和個人」。

「當今數據跨境流動已經成為經濟全球化的前提，是推進「一帶一路」建設的必要條件，我們願同各國就此問題開展交流合作，共同促進數據依法有序自由跨境流動，充分保障個人信息安全和國家網絡安全」。

此外，網安法還重點提出了要加強對公民個人信息的保護，防止公民個人信息數據被非法獲取、泄露或者非法使用。針對公民個人信息保護領域，最高法、最高檢作出了辦理侵犯公民個人信息刑事案件司法解釋，明確了「公民個人信息」的定義，並規定非法獲取、出售或者提供行蹤軌跡信息、通信內容、財產信息50條以上的即可入罪。

来源：香港大公报 2017-06-01

香港的优势



「香港的优势难以替代...
如自由开放的体制、便利的
营商环境、广泛的国际联系、
发达的服务业、先进的基础设施、国际接轨的法治、
自由流通的資訊以及众多的高素质人才...」
— 中共中央政治局常委、全国人大常委会委员长
张德江先生2016年5月18日出席香港「一带一路高峰论坛」演讲

经贸与个人信息

- 经贸数码化
- 大数据时代
- 人工智能
- 信息带动经济



信息资讯自由流通、 利便投资、营商

- 个人信息、数据
- 跨越不同的边境
- 国际信息流的法律限制



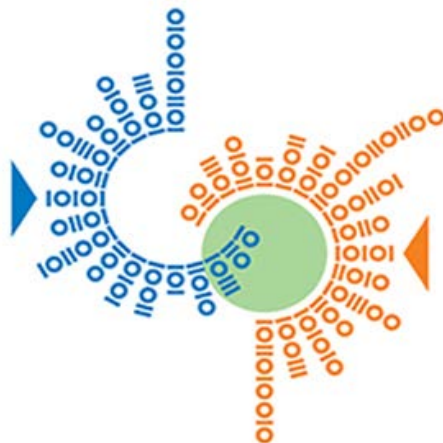
香港的作为数据中心的优势

- 数据中心的**首选地点**
- 2016 年「云端计算准备充足指数」
整体**排名第一**：
 - 国际連通性 #1
 - 数据中心安全性 #1
 - **隐私保障 #1**
 - 宽带质量 #2
 - 电网稳定性 #2



香港 – 「五流」匯聚之地

- 人才流
- 物流
- 資金流
- 服務流
- 信息資訊流



香港健全的法律制度

- 法治精神
- 普通法司法管辖区
- 严谨的商业法和财产法
- 办理业务合约、各类纠纷
- 信誉良好的司法机构
- 国际仲裁中心



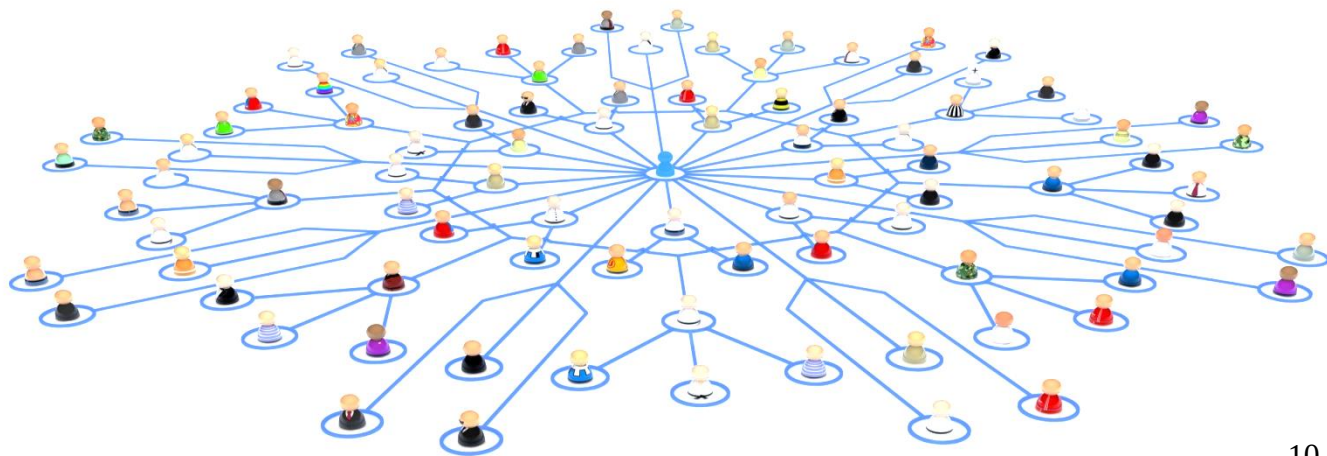
香港 – 信息资讯流

- 保护个人信息
- 信息自由流通
- 平衡点
- 信任



何謂个人信息?

- 识别该个人身份之信息
- 包括消费者的信息



全球个人信息保障的发展

1973	瑞典（全球首部个人信息保障法律）
1980	OECD《私隐指引》
1981	欧洲议会（Council of Europe）个人信息保障公约（Convention 108）
1995	欧盟《资料保障指令》
1995	香港《个人资料（私隐）条例》
2005	APEC《亚太经济合作组织私隐保障纲领》（APEC Privacy Framework）
2013	OECD 修正《私隐指引》
2016	欧盟《通用数据保护条例》

亚洲中最早订立、 单一和完整的个人信息保障法律

- 亚洲首个司法管辖区就个人信息制订全面的保障法例
- 全面、独立
- 公、私营机构



香港信息、数据保障制度紧贴全球标准

- 条例建基于国际认可的保障资料原则
- 参照OECD 及欧盟标准
- 适时的法例改革



香港《个人资料（私隐）条例》

- 六项「保障资料原则」，涵盖个人信息由产生到销毁的整个生命周期，即：

- o 第1原则：收集目的及方式
- o 第2原则：准确性及保存期
- o 第3原则：使用（包括披露及转移）
- o 第4原则：信息保安
- o 第5原则：政策及透明度
- o 第6原则：查阅及更正



六項保障資料原則簡介短片

1 收集目的及方式



資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

2 準確性、儲存及保留



資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

3 使用



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

4 保安措施



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

5 透明度



資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

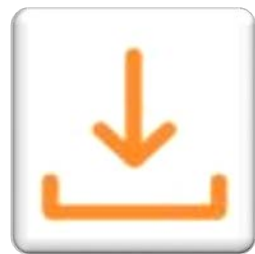
6 查閱及更正



資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

原则 1 — 收集资料的目的及方式

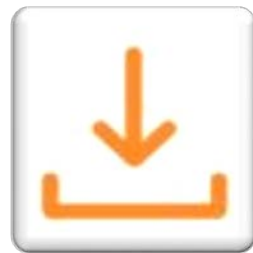
- 必须与资料使用者的职能或活动有关
- 收集的方式必须合法及公平
- 收集的资料要适量而不过多



原则 1 — 收集资料的目的及方式

收集个人资料声明

- 有效向资料当事人沟通，考虑因素包括「收集个人资料声明」的设计及表达方式、使用的语言等
- 清楚说明资料使用目的及资料承让人类别



原则 1 — 收集资料的目的及方式

收集个人资料时，须告知资料当事人以下五项资讯：

(a) 收集资料的目的；

(b) 资料可能会转移给什么类别的人；

收集个人资料
声明 (PICS)



(c) 资料当事人是否有责任抑或是可自愿提供资料；

(d) 如资料当事人有责任提供该资料，他拒绝提供资料所需承受的后果；及

(e) 资料当事人有权要求查阅及要求改正自己的个人资料，及提供处理有关要求的人士的职衔及地址。

收集个人资料
声明 (PICS)

原则1：案例—收集指纹资料



- 高级时装公司要求员工提供**指纹资料**以用作保安及员工考勤（私隐专员的调查报告编号：R15-2308）
- 调查结果：公司收集指纹资料属**过度**，收集方式属**不公平**
- 原因：
 - 指纹属敏感个人资料
 - **过度收集**：公司已有其他较不侵犯隐私的方法以达致保安及考勤目的，例如：
 - 公司已於出入口装设了保安摄录机、密码锁、链锁以作保安
 - 员工考勤可用智能卡
 - **不公平收集**：公司与员工之间地位不对等；员工没指纹以外的其他选择

原则 2 一个人资料的准确性及保留时限

- 资料使用者须采取切实可行的步骤，确保所持个人资料的准确性，及在完成资料的使用目的后删除资料
- 如资料使用者聘用资料处理者处理个人资料，须透过合约规范或其他方法，防止转移的资料被保存超过处理资料所需时间



原则2：案例 (1) — 保存破产资料

- 银行保留破产人士资料长达99年
(私隐专员的调查报告编号：R11-6121)
- 调查结果：银行保留资料的时间过长
- 原因：
 - 根据《破产条例》，破产人士在4至8年内会获解除破产
 - 银行保留破产资料不应超过8年
 - 长期保留破产资料或会不当地标签有关人士

原则2：案例 (2) — 税务局的纳税人地址不准确

- 税务局错误地更改了一名纳税人的通讯地址
(私隐专员的调查报告编号：R11-11778)
- 背景：
 - 一名税务局职员将纳税人甲的更改地址表格错误地夹附於纳税人乙的档案中
 - 其后另一名税务局职员根据纳税人甲的更改地址表格更改纳税人乙档案中的通讯地址，期间没有核对有关表格及档案的编号是否一致
 - 其后纳税人乙的税单因无法成功派递而被退回予税务局，但局方仍未能还原纳税人乙的正确地址，致令纳税人乙的税单被三次寄到错误的地址并且没有被退回
- 调查结果：税务局没有采取切实可行的措施以确保资料准确

原则 3 个人资料的使用

- 如无当事人的订明同意，个人资料不得用于新目的

「**新目的**」指在收集资料时拟使用的目的或
直接有关的目的以外的目的



原则3：案例—外佣中介网上展示资料

- 雇佣中介公司于网上披露外籍佣工的姓名、住址、护照号码、家庭背景等资料，任由公众人士查阅
(私隐专员的调查报告编号：R14-1382)
- 调查结果：中介公司过度披露个人资料
- 原因：
 - 上述资料无助准雇主挑选合适佣工
 - 网上公开有关资料不必要地增加了外籍佣工的隐私风险

原则 4 一个人资料的保安

- 资料使用者须采取切实可行的步骤，保障个人资料不会被未获授权或意外的查阅、处理、删除、丧失或使用
- 如资料使用者聘用资料处理者处理个人资料，须透过合约规范或其他方法，以保障转移的个人资料



原则4：案例一选举事务处遗失电脑

- 政府部门在特首选举的后备场地**遗失一台手提电脑**，当中载有全香港378万名选民的个人资料，包括敏感的**身份证号码**
(私隐专员的调查报告编号：R17-6429)
- 调查结果：政府部门没有采取所有合理地切实可行的步骤，确保选民的个人资料安全
- 原因：
 - 特首选举只有1,200 名选委有权投票，无须带备全香港378万名选民的个人资料
 - 部门没有就在特首选举中以电脑储存选民的个人资料制订清晰的政策及指引
 - 用於加密电脑内的资料的密码过於简单
 - 存放电脑的房间保安措施不足，例如保安摄录机并不覆盖房间出入口

原则4：其他资料保安不足的案例

- 某公司错误地将载有1,880名客户的个人资料档案以电邮发送予第三者，而有关档案亦没有加密
- 某保险公司网页存取权限设置错误，以致600份保单外泄
- 某律师行委托派递员将一份离婚文件派送到当事人的办事处，但并没以信封装载有关文件，以致曾经手派送及接收文件的人士可阅览当中内容
- 某医院遗失病人的病历档案，私隐专员介入后得悉医院并没有系统地记录病历档案的流向

原则 5 — 资讯须在一般情况下可提供

资料使用者须提供：

- (a) 处理个人资料的政策及实务；
- (b) 持有的个人资料的种类；
- (c) 会为何种主要目的而使用资料



原则5：案例—隐蔽式摄录机

- 某机构在办公室安装**隐蔽式摄录机**以调查是否有员工监守自盗（私隐专员的调查报告编号：R05-7230）
- 调查结果：机构违反有关隐私政策透明度的规定
- 原因：
 - 受影响的员工对被摄录机监察**毫不知情**
 - 机构没有制订与监察员工有关的**私隐政策**



原则 6 – 查阅个人资料

- 资料当事人有权要求查阅及改正自己的个人资料
- 资料使用者可收取不超乎适度的费用
- 资料使用者要在40天内遵从



31

原则6：案例—查阅资料收费

- 员工向雇主提出查阅资料要求，索取一份有关他工作表现评核报告的复本，雇主就四页纸的评核报告，以划一收费（每页港币50元），向员工收取合共200港元。
（私隐专员的个案简述参考编号：2015C02）
- 调查结果：雇主的**收费过高**
- 原因：
 - 资料使用者只可向要求者收取跟依从查阅资料要求「直接有关及必需」的费用, 不应以商业准则收取费用
 - 雇主未能提供厘订划一收费(即每页50港元)的基础
 - 雇主未能证明200港元金额是为依从查阅资料要求的成本

资料转移境外

- 私隐条例**第33条**禁止（除非在指定情况下）将个人资料转移至香港以外的地区
- 指定情况包括：
 - 得到资料当事人的同意
 - 有关目的地具备与香港相约的个人资料保障
 - 转移资料的一方已采取合理措施以保障被转移的资料
- **第33条尚未实施**，但纵使有关资料已被转移至香港以外地区，如该资料使用者能够在 / 从香港控制有关资料的持有、处理或使用，则仍须遵从私隐条例的规定，包括：
 - **第3原则**规定资料使用者不得使用资料於新目的，除非事先获得资料当事人明确及自愿的同意；
 - **第2(3)及第4(2)原则**规定资料使用者要采取合约规范方法或其他方法，以确保其资料处理者（不论是在香港或香港以外聘用）不会保留资料过久，及采取足够的资料保安措施
 - **第65条**订明资料使用者须为其员工及代理人的违法行为负责

私隐专员的执法权

- 违反保障资料原则**并非**刑事罪行
- 私隐专员有权向违反保障资料原则的人士发出「**执行通知**」，指令有关人士作出改正行动
- 不遵从「执行通知」属刑事罪行，一经法院定罪，可判罚款港币50,000元及判囚两年
- 违反私隐条例的其他规定（例如直接促销）可能构成刑事罪行
- 违反私隐条例中有关直接促销的规定最高可判罚款港币一百万元及判囚五年
- 私隐专员无权进行刑事调查或公诉，但可将案件转介予警察

区外联系

- 亚太区私隐机构
(委員)



- 亚太经济合作组织 -
电子商贸督导小组
资料私隐分组



- 国际资料保障及私隐专员研讨会
(委員)



- 全球私隐执法机关网络
(委員)



- 「保障个人资料」国际会议

- 电讯资料保障国际工作小组

Hong Kong Looks to Take a Global Privacy Leadership Role

Facebook Twitter LinkedIn YouTube

This fall, at the end of September, the International Conference of Privacy and Data Protection Commissioners will kick off in Hong Kong, bringing the world's regulators together for the 39th time. It's no coincidence that Hong Kong will play host. In Privacy Commissioner for Personal Data Stephen Wong, Hong Kong has a motivated and active privacy enforcer looking to be a leader on the global stage.

Of course, Hong Kong has long been a leader in the Asia-Pacific region, with one of the oldest privacy frameworks in the region. The PCPD, as the regulator, has been busy with workshops, issuing statements, and increasingly producing guidance for organizations looking to operate in Hong Kong.

In 2016, alone, the PCPD conducted 255 personal workshops, with 35,000 participants. The regulator has also issued 21 publications, and 18 large-scale promotional events for the general public are extremely out of the ordinary for a privacy commissioner's office. They even put together a "privacy episode" series. This is an organization that's laying the groundwork for no-excuses enforcement. Every effort has been made to let you know how privacy should be done. Violate it, and you're on your own risk.

One specific thing to remember about Hong Kong's privacy regime is that violating privacy rules can be a crime in Hong Kong, and that the PCPD actually refers cases to the police for prosecution. In 2016, the PCPD referred 10 privacy-related crimes, all for direct marketing without consent, basically resulting in fines and industry sanctions.

Quite simply, it's not just your company that could suffer, but perhaps your reputation.

This is relatively rare, however, and the Hong Kong Commissioner's office, like Singapore, prides itself on being a hub of global business, and a place where privacy enforcement with making sure regulations aren't too onerous.

So, what's likely to actually land you in hot water? For one, standing out from the crowd. When's office has appealed to corporations to "self-regulate" by providing transparent privacy statements and policies. What's your privacy statement says you're going to do, and what you're actually doing. Direct marketing has been most significantly in the past, or even direct marketing.

Hong Kong residents do not like spam of any kind and the Commissioner stemmed from direct marketing, and it's a good thing.

There is also growing awareness of Hong Kong's privacy ordinance, and the Commissioner has received a significant number of complaints to the Commissioner involving the financial sector. Hong Kong consumers are savvy.

It might also be instructive to look at the PCPD's areas of focus from 2016:

- CCTV. Yes, they still call it that, even though not many cameras run on the coaxial cable anymore. If you're putting a camera somewhere, make sure you provide notice, have a policy for who can view the footage, and keep security tight. If footage you captured gets out into the light of day, that's a serious breach in Hong Kong.
- Mobile apps. Along with many other global privacy commissions, the PCPD has expressed specific concerns about the personal nature of the data collected on mobile devices. Specifically, make sure you're transparent about collecting location data or accessing things like a device's camera or microphone. And make sure you use just-in-time notices, not simply a line or two buried in the app's privacy notice. That won't cut it.
- Internet of Things. Similar to mobile apps, the IoT devices, like fitness trackers or virtual assistants, have access to vast amounts of personal data. The Commissioner has expressed concern about how manufacturers can provide notice in areas where there is often no screen or other way for users to read privacy notices in a traditional way. Be overly transparent if there's any question about whether users might not expect certain data to be collected or used.

All of that said, the PCPD issues more warnings than enforcement actions. However, in a highly competitive market like Hong Kong, it may be that the brand-hit that comes with a warning could be almost as damaging as a fine or other action. Especially given the regulators willingness to listen and provide advice, it seems especially prudent to err on the side of caution and communicate with the PCPD if you're considering an innovative use of data on the island.

Tags: API, Privacy

Posted on May 4, 2017



by Sam Pfeifle

Content Director, International Association of Privacy Professionals

Source: <https://www.rsaconference.com/blogs/hong-kong-looks-to-take-a-global-privacy-leadership-role>

香港将扮演全球信息资料 私隐保障领导角色

“...香港一直以来
是亚太区的领导，
在区内率先制定保
障信息私隐框架”



est. 1996

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

欧盟 《通用数据保护条例》 (GDPR)



- 2016年5月通过
- 2018年5月实施
- 取代1995欧盟指引
- 第 3 条：境外执法权
 - 即使机构在欧盟境内没有业务单位，只要企业向欧盟的居民提供产品和服务（例如通过网络），或对欧盟居民的行为进行监察（例如网络监控），亦须遵守欧盟的新条例
- 第44-47条：个人信息转移至欧盟以外地区的限制
- 第83条：行政罚款（最高罚款为 2千万欧罗或企业全球年营业额百分之四的金额）



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

- ☐ 查詢電話
- ☐ 傳真
- ☐ 網址
- ☐ 電郵
- ☐ 地址

2827 2827

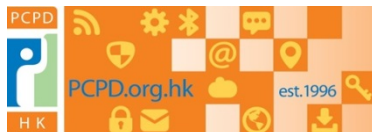
2877 7026

www.pcpd.org.hk

enquiry@pcpd.org.hk

香港灣仔皇后大道東248號
陽光中心12樓

謝謝！



香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong