



內地民商事務所涉 個人信息及網絡安全 主要法規簡介

PCPD



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



內地民商事務所涉個人信息 及網絡安全主要法規簡介





免責聲明

本簡介所載的資訊和建議只作一般參考用途，並非為本簡介內所提述的法規的應用提供詳盡指引。有關法規的詳細及明確內容，請直接參閱有關法規的本文。個人資料私隱專員（「私隱專員」）及洪延青博士並沒有就本簡介內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。此外，中國內地涉及保護個人信息的法規的數目眾多，並且不時作出更新。此簡介只涵蓋了部分相關的法規，並只按有關法規於2019年11月22日為止的最新版本或最新草案作為基礎。此簡介並不涵蓋任何在2019年11月22日後對有關法規或草案作出的更新或修訂。個別機構或人士為符合中國內地有關保護個人信息的規定，應尋求專業的法律意見。



目錄

鳴謝	1
序言	2
(一) 背景	5
(二) 憲法保障	7
(三) 刑法規定	9
(四) 民事保障	12
(五) 消費者權益保障	15
(六) 《網絡安全法》及其相關法規	17
(1) 《網絡安全法》	17
(2) 《數據安全管理辦法》(徵求意見稿)	21
(3) 《個人信息出境安全評估辦法》(徵求意見稿)	25
(4) 《兒童個人信息網絡保護規定》	28
(5) 《個人信息安全規範》(徵求意見稿)	30
(6) 《網絡安全威脅信息發布管理辦法》(徵求意見稿)	34



(七) 《電子商務法》	37
(八) 其他行政法規、部門規章和指引	39
(1) 《銀行業金融機構數據治理指引》	39
(2) 《移動互聯網應用程序信息服務管理規定》	40
(3) 《移動互聯網應用(App)收集個人信息基本規範》(草案)	41
(九) 結語	43
附錄1 — 內地有關個人信息保障法規的訂立時間表	44
附錄2 — 內地個人信息保障法規簡覽	46
附錄3 — 香港《個人資料(私隱)條例》與內地保障個人信息 相關法規的比較	47



特此鳴謝為此簡介提供專業意見及指導的洪延青博士：

洪延青博士現任北京大學法治與發展研究院高級研究員，主要研究個人信息保護、數據跨境流動、關鍵信息基礎設施保護及網絡安全等法律政策議題。洪博士目前亦兼任世界經濟論壇網絡安全全球未來理事會委員(2018至2019年)。洪博士曾任職於國家互聯網信息辦公室，在網絡安全戰略、政策及法規制定方面具有豐富經驗，並曾參與一系列重大網絡安全政策、法規的起草工作。洪博士亦曾擔任全國信息安全標準化技術委員會2016年重點標準制定專案《個人信息安全規範》編制組組長，以及2017年重點標準制定專案《資料出境安全評估指南》編制組副組長。

序言

在科技迅速發展的背景下，以大數據、雲端計算、人工智能等為代表的科技正逐漸改變着我們的生活與工作模式，並對個人信息隱私帶來影響。同時，在大數據背景下，個人信息的價值越來越高，亦令社會上滋生了新型的個人信息相關的犯罪。因此，嚴格保護個人信息的法規越來越重要。

世界各國對於個人信息保護的立法模式大致可分為兩大類，即「分散立法模式」和「統一立法模式」。「分散立法模式」以美國為典型，即逐一在各個領域立法。「統一立法模式」可以香港為例，是一部全面的個人信息保護法律。目前中國內地針對個人信息保護方面的規管分散於多部法律、行政法規、部門規章和指引等規範性文件中，有關監管框架也在不斷擴張。自從2013年中國內地推出首個個人信息保護國家標準——《信息安全技術公共及商用服務信息系統個人信息保護指南》，界定何謂「個人信息」以來，為保護個人信息而修訂或制定的法規開始不斷湧現，例如《消費者權益保護法》、《刑法》、《網絡安全法》、《電子商務法》、《兒童個人信息網絡保護規定》、《個人信息安全規範》等，針對在中國內地開展個人信息收集、存儲、傳輸、處理、使用等活動作出具體規定。最高人民法院及最高人民檢察院於2017年聯合頒布的《關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》，明確地指出何謂《刑法》中的「違反國家有關規定」處理個人信息，並對侵犯個人信息相關罪行的量刑準則提供指引，有效解決了有關法律在應用時可能發生的爭議。其他可能即將陸續生效的法規還有《數據安全管理辦法》、《個人信息出境安全評估辦法》、《移動互聯網應用（App）個人信息基本規範》等。

內地執法及監管機構在執行個人信息保護法規方面亦不鬆懈。例如在2014年8月，兩名外國公民所經營的公司因非法收集、購買及轉售與中國公民相關的私人信息，被法院判處有期徒刑及處以大額罰款。2018年初，一家內地龍頭網絡平台因違規收集消費者個人信息而被起訴，直至其全面移除所有侵犯個人隱私的功能技術軟件，案件才完結。2019年1月，國家互聯網信息辦公室、工業和信息化部、公安部、市場監管總局聯合展行「App違法違規收集使用個人信息專項治理」，嚴厲查處各類違法違規行為，並務求強化行業自律。

以上的事件代表著中國內地正從刑事及行政手段加強對個人信息的保護。此外，中國內地亦開始著重將隱私權及個人信息權視為獨立的人格權，並賦予民事保障。例如繼2010年實施的《侵權責任法》確認公民享有民事的隱私權益後，2017年實施的《民法總則》及2019年發布的《民法典人格權編（草案三次審議稿）》進一步深化個人在隱私權及個人信息權方面的保障。

2019年3月，在第十三屆全國人民代表大會二次會議期間，大會的外事委員會主任委員表示已將《個人信息保護法》列入本屆立法規劃，並爭取早日出台。可以預見有關法律出台後，中國內地的個人信息保護將會再一次大大提升。

隨著各種法規的出台，社會大眾的隱私和個人信息受到更廣泛及更大程度的保障。然而，由於中國內地關乎個人信息保護的法規眾多，期待到這個新興市場擴展業務的企業須面對符規方面的挑戰。本人希望藉著本簡介，幫助各個與內地有聯繫或業務往來的機構、企業掌握有關內地法規，從而對推動粵港澳大灣區的發展作出微薄的貢獻。本人特別希望此簡介能成為創新科技企業的「工具箱」，幫助他們在發展和運用大數據、雲端計算、人工智能等技術時邁向成功。

在2019年秋末，於阿爾巴尼亞地拉那舉行的第四十一屆國際資料保障及私隱專員會議（現易名為「環球私隱議會」）上，通過了以發展「全球趨向一致的信息保障法律」為使命，希望從而促進個人信息安全、順暢地跨境流動。本人殷切期盼藉著本簡介，促進香港及其他地區對中國內地個人信息保護法規的認識，提升全球個人信息保障監管框架的相互可操作性，以及促進數據跨境流動及數據經濟發展。

本簡介只供一般參考用途，而非有關法規的符規指引。各機構或人士若要符合內地有關規定，應尋求專業的法律意見。

黃繼兒大律師

香港特別行政區個人資料私隱專員

二零一九年十一月

(一) 背景

1. 中國內地目前並未有一套全面的個人信息保護法，對個人信息的保障現分散於不同的法律、行政法規、部門規章和指引等規範性文件(以下統稱「法規」)，情況與香港的單一、全面的個人信息保護法例(即香港法例第486章《個人資料(私隱)條例》)有別。然而，中國內地正不斷建設和完善個人信息和隱私權相關的法律。此外，各政府部門和監管機構亦相繼推出了部門規章和指引等，以落實和補充相關法律要求。
2. 內地目前亦未有專責部門負責執行保護隱私及個人信息的法規，有關執法權力分散於各政府部門。例如《網絡安全法》的執法部門包括公安部、工業和信息化部(「工信部」)、國家互聯網信息辦公室(「網信辦」)，以及相關行業主管部門。
3. 國家主席習近平於2019年9月就天津舉行的「國家網絡安全宣傳周」作出重要指示，當中強調國家網絡安全工作包括保障個人信息，以及維護公民在網絡空間的合法權益。習近平同時強調要堅持促進科技產業發展和依法管理相統一，既大力培育人工智慧、物聯網、下一代通信網絡等新科技、新應用，亦要積極利用法規引導新科技應用¹。因此，我們預期中國內地有關保障個人信息及網絡安全的法規將會愈趨嚴謹和細緻。

1 資料來源：新華社(2019年9月16日)



憲法保障



(二) 憲法保障

4. 《中華人民共和國憲法》列明公民的人格尊嚴不受侵犯²，禁止非法搜查或者非法侵入公民的住宅³，以及確保公民的通信自由和通信秘密受法律的保護⁴。此是中國內地公民的隱私權和個人信息保護權的根本來源。

2 《中華人民共和國憲法》第38條

3 《中華人民共和國憲法》第39條

4 《中華人民共和國憲法》第40條

(三) 刑法規定

5. 《刑法修正案(九)》於2015年11月1日起實施，當中就保護公民個人信息方面作了特別規定，包括將竊取或以其他不法方式取得公民個人信息，以及在「違反國家有關規定」的情況下出售或提供公民個人信息列為刑事罪行。就情節嚴重的個案，違法者一經定罪，最高可處三年以下有期徒刑及罰款。至於情節特別嚴重的，可處三年以上、七年以下有期徒刑及罰款⁵。
6. 就《刑法》中有關侵犯公民個人信息的罪行的涵蓋範圍及量刑標準等，最高人民法院及最高人民檢察院聯合公布了若干解釋⁶，並於2017年6月1日起施行。解釋中提出「公民個人信息」是指「以電子或者其他方式記錄的能夠單獨或者與其他信息結合識別特定自然人身份或者反映特定自然人活動情況的各種信息，包括姓名、身份證件號碼、通信通訊連絡方式、住址、帳號密碼、財產狀況、行蹤軌跡等。」上述「公民個人信息」的定義比香港《個人資料(私隱)條例》下的「個人資料⁷」的定義更廣，尤其公民個人信息包括「反映特定自然人活動情況的各種信息」及「行蹤軌跡」。解釋亦說明《刑法》中的「違反國家有關規定」是指「違反法律、行政法規、部門規章有關公民個人信息保護的規定」。此外，解釋亦列舉了「情節嚴重」和「情節特別嚴重」的罪行情況。例如出售或者提供行蹤軌跡信息予他人用於犯罪的屬情節嚴重；造成被害人死亡、重傷、精神失常或者被綁架等嚴重後果的，屬情節特別嚴重。

5 《刑法》第253(1)條

6 《最高人民法院 最高人民檢察院關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》

7 《個人資料(私隱)條例》第2(1)條訂明，「個人資料」是指直接或間接與一名在世的個人有關的資料，並且從該資料直接或間接地確定有關的個人的身分是切實可行的，以及該資料的存在形式令予以查閱及處理均是切實可行的。

案例

中國最高人民檢察院於2017年5月發布了六宗有關侵犯公民個人信息罪的典型案例，以警醒社會公眾遵紀守法、提高司法保護意識，並為各地檢察機關辦理相關案件提供指引、參考。案例中的犯人一般通過工作便利、惡意電腦程式、詐騙或購買等方式非法獲取公民個人信息，然後轉售圖利。據有關案例，犯人一經定罪，通常被處以有期徒刑及罰款。

例如在一宗2016年3月上海市黃浦人民法院的案件中，其中一名被告利用惡意程式盜取了一個網站的顧客的個人信息12,000多條，然後轉售獲利人民幣5,000多元，結果被判有期徒刑一年零九個月，並罰款人民幣50,000元。

2017年2月，上海市浦東新區人民法院的一宗案件中，在上海市疾病預防控制中心工作的一名被告聯同另外七人，利用工作便利，取得上海市新生嬰兒的個人信息共30萬條，然後轉售圖利，結果八人被判有期徒刑七個月至兩年零三個月不等。

(四) 民事保障

7. 於2010年7月1日實施的《侵權責任法》已確認公民享有民事的隱私權益，奠定了個人信息保護的民事制度基礎⁸。此外，《民法總則》於2017年10月1日起實施，補充已有的《民法通則》，全面系統地確立了內地民事活動的基本規定。就民事權益方面，《民法總則》重申公民享有隱私權⁹，並列明公民的個人信息受法律保護¹⁰。任何組織和個人需要獲取他人的個人信息，應當依法取得並確保信息安全，不得非法收集、使用、加工、傳輸他人的個人信息，不得非法買賣、提供或者公開他人的個人信息。違反《民法總則》要承擔民事責任，當中包括停止侵害、賠償損失、消除影響、恢復名譽及賠禮道歉¹¹。

8. 全國人民代表大會常務委員會於2019年8月28日公布《民法典人格權編(草案三次審議稿)》，向社會公眾徵求意見。《民法典》為《民法總則》的延伸，就民事事宜作出更細緻的規定。有關草案的第六章再次重申個人的隱私權和個人信息受法律保護，並將隱私定義為「自然人不願為他人知曉的私密空間、私密活動和私密信息等¹²」。有關草案亦明確列出收集和處理個人信息的原則和規定(當中與本簡介第六部介紹的規定類近)，包括¹³：
 - (a) 遵循合法、正當、必要原則收集和處理個人信息；
 - (b) 收集和處理個人信息時要徵得有關個人或者其監護人同意；
 - (c) 公開收集、處理個人信息的規則；
 - (d) 明示收集、處理個人信息的目的、方式和範圍；
 - (e) 不違反法律、行政法規的規定和雙方的約定收集或處理個人信息；
 - (f) 容許個人查閱、更正及刪除其個人信息；及
 - (g) 採取措施確保個人信息安全。

8 《侵權責任法》第2條

9 《民法總則》第110條

10 《民法總則》第111條

11 《民法總則》第179條

12 《民法典人格權編(草案三次審議稿)》第811條

13 《民法典人格權編(草案三次審議稿)》第814至第817條

案例

北京市第一中級人民法院於2017年3月審理了一宗涉及洩露個人信息的民事上訴案件。原告人經一網上中介平台訂購機票後不久收到了訛稱有關航班取消的詐騙電話訊息，因而控告有關航空公司及中介平台（以下統稱「被告」）洩露其個人信息及侵犯其隱私權，並要求被告賠償他的精神損害。一審法院認為原告人未能提供足夠證據證明被告洩露其個人信息而判原告人敗訴。經上訴後，北京市第一中級人民法院認為一審法院對原告人舉證責任的要求太高。雖然被告可能並非掌握原告人涉案的個人信息的唯一機構，但考慮到涉案的詐騙訊息的內容，以及當時多家媒體機構都曾報導過被告懷疑洩露乘客的信息等，中級人民法院認為有高度可能是被告洩露原告人的個人信息，改判原告人勝訴。然而，中級人民法院只要求被告於其網頁向原告公開道歉，並駁回原告人的賠償要求。

有內地法律界評論認為此案有兩大重點須留意：（1）法院承認要原告人證明其個人信息外洩的源頭有困難，因而願意就此接受較低的舉證門檻；（2）就索取賠償，法院依然遵從一貫原則，要求被告能證明受到損害。

(五) 消費者權益保障

9. 《消費者權益保護法》於2013年10月作出了第二次修正，當中加入了對消費者的個人信息的保障。有關修訂於2014年3月15日起施行。經修訂後的《消費者權益保護法》列明，消費者在購買、使用商品和接受服務時，享有個人信息依法得到保護的權利¹⁴。此外，《消費者權益保護法》對經營者如何處理和保護消費者的個人信息亦有較明確的規定，包括：
- (a) 收集、使用消費者個人信息，應當遵循合法、正當、必要的原則，明示收集、使用信息的目的、方式和範圍，並經消費者同意；
 - (b) 公開收集及使用個人信息的規則；
 - (c) 嚴格保密消費者的個人信息，不得洩露、出售或者非法向他人提供；
 - (d) 採取措施確保個人信息安全，防止個人信息外洩；
 - (e) 在發生或者可能發生信息洩露、丟失的情況時，應當立即採取補救措施；及
 - (f) 未經消費者同意，不得向其發送商業性信息¹⁵。
10. 《消費者權益保護法》禁止經營者以格式條款、通知、聲明、店堂告示等方式，作出排除或者限制消費者權利、減輕或者免除經營者責任、加重消費者責任等對消費者不公平、不合理的規定，否則有關條款所列的相關內容將會無效¹⁶。
11. 若經營者侵害消費者的個人信息依法得到保護的權利，應當停止侵害、恢復消費者的名譽、消除對消費者的影響、賠禮道歉，並賠償損失¹⁷。此外，經營者亦可能被處以警告、沒收違法所得(如有)及罰款。情節嚴重的，經營者可被責令停業整頓，甚或吊銷營業執照¹⁸。

14 《消費者權益保護法》第14條

15 《消費者權益保護法》第29條

16 《消費者權益保護法》第26條

17 《消費者權益保護法》第50條

18 《消費者權益保護法》第56(9)條



《網絡安全法》及其相關法規



(六) 《網絡安全法》及其相關法規

(1) 《網絡安全法》

12. 《網絡安全法》於2017年6月1日開始實施，其立法目的包括保障網絡安全、社會公共利益和公民的合法權益，以及維護網絡空間主權和國家安全¹⁹，主要監管對象為在中國內地建設、營運、管理、維護或使用網絡的「網絡運營者」²⁰。「網絡運營者」並不限於經營互聯網相關業務的機構，亦包括其他利用信息網絡銷售產品或提供服務的機構，例如零售商店、酒店、航空公司及銀行等。《網絡安全法》第四章對網絡運營者收集及處理個人信息有較全面而概括的規定。

個人信息的定義

13. 《網絡安全法》中「個人信息」是指「以電子或者其他方式記錄的能夠單獨或者與其他信息結合識別自然人個人身份的信息，包括但不限於自然人的姓名、出生日期、身份證件號碼、個人生物識別信息、住址、電話號碼等²¹。」上述定義與最高人民法院及最高人民檢察院的聯合解釋相近，但較解釋的定義狹窄，因解釋的定義還包括「反映特定自然人活動情況的各種信息」。



19 《網絡安全法》第1條

20 《網絡安全法》第2及76(3)條

21 《網絡安全法》第76(5)條

個人信息保護規定

14. 在保護個人信息方面，《網絡安全法》對網絡運營者有以下的規定²²：

- (a) 嚴格保密個人信息，並建立健全個人信息保護制度；
- (b) 收集、使用個人信息，應當遵循合法、正當、必要的原則；
- (c) 公開收集、使用個人信息的規則；
- (d) 明示收集、使用個人信息的目的、方式和範圍，並取得被收集者(個人)的同意；
- (e) 不得收集與提供的服務無關的個人信息；
- (f) 收集、使用個人信息時不得違反法律、行政法規的規定，或與有關個人的約定；
- (g) 不得洩露、篡改、毀損其收集的個人信息；
- (h) 未經有關個人同意，不得向他人提供個人信息(經過處理而無法識別特定個人且不能復原的除外)；
- (i) 採取技術措施和其他必要措施，確保個人信息安全，防止信息洩露、毀損、丟失；及
- (j) 在發生或者可能發生個人信息洩露、毀損、丟失的情況時，立即採取補救措施，按照規定及時告知使用者並向有關主管部門報告(須留意《網絡安全威脅信息發布管理辦法》的規定；詳見本簡介第六(6)部)。

22 《網絡安全法》第40至42條

更正及刪除個人信息

15. 《網絡安全法》賦予個人(作為個人信息主體)以下權利²³：
- (a) 若發現網絡運營者違反法律、行政法規的規定或者雙方的約定收集、使用其個人信息，有權要求網絡運營者刪除其個人信息；
 - (b) 若發現網絡運營者收集、存儲的其個人信息有錯誤的，有權要求網絡運營者予以更正，而網絡運營者應當採取措施予以刪除或者更正。

非法獲取或出售個人信息

16. 《網絡安全法》禁止任何個人和組織竊取或者以其他非法方式獲取個人信息，或以非法方式向他人出售或提供個人信息²⁴。

出境限制

17. 《網絡安全法》對個人信息及重要數據的出境作出限制，當中規定「關鍵信息基礎設施」的運營者在中國內地運營中收集和產生的個人信息和重要數據須在內地儲存²⁵。「關鍵信息基礎設施」包括公共通信及信息服務、能源、交通、水利、金融、公共服務、電子政府，以及其他重要行業和領域²⁶。如因業務原因而確實須要向境外提供個人信息或重要數據，應當按照國家網信部門會同國務院有關部門制定的辦法進行安全評估(詳見本簡介第六(3)部)。

23 《網絡安全法》第43條

24 《網絡安全法》第44條

25 《網絡安全法》第37條

26 《網絡安全法》第31條

罰則

18. 網絡運營者如違反上述《網絡安全法》的規定，可被責令改正，並根據情節嚴重程度而處以警告、沒收違法所得（如有）、處以罰款（最高為違法所得的十倍或 100 萬元）、對直接負責的主管人員和其他直接責任人員處以最高 10 萬元罰款，甚或責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或營業執照。如構成犯罪的，依法追究刑事責任²⁷。

治理行動

有見於移動互聯網應用程式強制授權、過度索權、超範圍收集個人信息的現象大量存在，違法違規使用個人信息的問題十分突出，網信辦、公安部、工信部及國家市場監督管理總局決定自 2019 年 1 月至 12 月，在全國範圍組織開展應用程式違法違規收集使用個人信息專項治理，確保相關運營者嚴格遵守《網絡安全法》、《消費者權益保護法》等的相關規定，包括：

- 遵循合法、正當、必要的原則，不收集與所提供服務無關的個人信息；
- 收集個人信息時要以通俗易懂、簡單明瞭的方式展示個人信息收集使用規則，並經個人信息主體自主選擇同意；
- 不以預設、捆綁、停止安裝使用等手段變相強迫使用者授權；及
- 不得違反法律法規和與使用者的約定收集、使用個人信息。

違規的運營者會被要求在限期內整改。逾期不改的，會被公開曝光。情節嚴重的，會被依法暫停相關業務、停業整頓、吊銷相關業務許可證或者吊銷營業執照。公安機關亦會依法嚴厲打擊針對和利用個人信息的違法犯罪行為。

19. 由於《網絡安全法》就個人信息的保護和數據出境的規定比較概括，內地有關當局因而草擬及制訂了一系列的行政法規和指引，協助機構落實《網絡安全法》的規定。有關行政法規和指引包括：
- (a) 《數據安全管理辦法》(徵求意見稿)；
 - (b) 《個人信息出境安全評估辦法》(徵求意見稿)；
 - (c) 《兒童個人信息網絡保護規定》；
 - (d) 《個人信息安全規範》；及
 - (e) 《網絡安全威脅信息發布管理辦法》(徵求意見稿)。

以下將逐一簡介上述行政法規和指引。

(2) 《數據安全管理辦法》(徵求意見稿)²⁸

20. 《數據安全管理辦法》適用於在中國內地利用網絡開展的數據收集、存儲、傳輸、處理、使用等活動，具法律約束力，對個人信息保障和重要數據安全管理提供較詳細的規定。



28 有關《數據安全管理辦法》的簡介是基於網信辦於2019年5月28日發布的徵求意見稿。截至2019年11月22日，《數據安全管理辦法》的正式版本仍未發布。

收集個人信息

21. 《數據安全管理辦法》規定網絡運營者利用網站或應用程式等收集個人信息時，要公開其收集及使用個人信息的規則。有關規則可包含於隱私政策中。規則須明確具體、簡單通俗及易於獲取，並且須包含以下內容²⁹：
- (a) 網絡運營者基本信息；
 - (b) 網絡運營者主要負責人、數據安全責任人的姓名及聯絡方式；
 - (c) 收集及使用個人信息的目的、種類、數量、頻度、方式、範圍等；
 - (d) 個人信息保存地點、期限及到期後的處理方式；
 - (e) 向他人提供個人信息的規則(如適用)；
 - (f) 個人信息安全保護策略；
 - (g) 個人信息主體撤銷同意，以及查詢、更正、刪除個人信息的途徑和方法；
 - (h) 投訴、舉報管道和方法；及
 - (i) 法律、行政法規另有規定的其他內容。
22. 網絡運營者在收集個人信息前，必先確保個人知悉並明確同意上述收集及使用個人信息的規則³⁰。網絡運營者不得以改善服務、提升用戶體驗、定向推送信息、研發新產品等為由，以默許、誤導、捆綁或強迫等方式取得個人的同意。網絡運營者亦不能以個人拒絕提供非必要的個人信息為由而拒絕提供核心功能或服務，或向個人採取歧視行為，例如服務質量和價格差異³¹。
23. 如個人信息的主體為14周歲以下的未成年人，有關個人信息的收集須得到其監護人的同意³²。

29 《數據安全管理辦法》(徵求意見稿)第7至8條

30 《數據安全管理辦法》(徵求意見稿)第9條

31 《數據安全管理辦法》(徵求意見稿)第11及第13條

32 《數據安全管理辦法》(徵求意見稿)第12條

收集個人敏感信息

24. 如網絡運營者收集個人敏感信息，須向所在地的網信部門備案。備案的內容包括收集及使用個人敏感信息的規則、目的、規模、方式、範圍、類型、期限等，但不包括信息內容本身³³。此外，網絡運營者亦須委任數據安全責任人，其職責包括組織制定數據保護計劃並督促其落實、組織開展數據安全風險評估、督促整改安全隱患、按要求向有關部門和網信部門報告數據安全保護和事件處置情況、處理個人投訴和舉報³⁴。

使用及披露個人信息

25. 網絡運營者使用個人信息時不得違反收集及使用規則。因業務需要，確需擴大個人信息使用範圍的，應當取得個人信息主體的同意³⁵。
26. 網絡運營者向他人提供個人信息前，應當評估可能帶來的安全風險，並取得個人信息主體同意，除非有關行為符合相關例外情況，例如有關披露明顯不違反個人信息主體的意願、信息已經過匿名化處理，或有關披露為對執法機關依法履行職責、維護國家安全、維護公眾利益等目的所必需³⁶。

保存期限

27. 網絡運營者保存個人信息不應超出收集使用規則中的保存期限，並於使用者注銷帳號後及時刪除或以匿名化處理其個人信息³⁷。

33 《數據安全管理辦法》(徵求意見稿)第15條

34 《數據安全管理辦法》(徵求意見稿)第17至18條

35 《數據安全管理辦法》(徵求意見稿)第22條

36 《數據安全管理辦法》(徵求意見稿)第27條

37 《數據安全管理辦法》(徵求意見稿)第20條

查詢、更正、刪除個人信息

28. 網絡運營者收到有關個人信息查詢、更正、刪除以及使用者注銷帳號請求時，應當在合理時間和收費予以查詢、更正、刪除或注銷帳號³⁸。

問責制

29. 網絡運營者應當參照國家相關標準，建立數據安全管理制度，制定數據安全計劃，實施數據安全技術防護（例如數據分類、備份、加密等）以保障數據安全，開展數據安全風險評估，制定網絡安全事件應急預案，及時處置安全事件，組織數據安全教育、培訓³⁹。

外洩通報

30. 當發生個人信息洩露、毀損、丟失等數據安全事件，或者當發生數據安全事件風險明顯加大時，網絡運營者應當立即採取補救措施，及時以電話、短信、郵件或信函等方式告知個人信息主體，並向行業主管監管部門和網信部門報告⁴⁰（須留意《網絡安全威脅信息發布管理辦法》的規定；詳見本簡介第六(6)部）。

個性化的定向推送信息

31. 如網絡運營者向個人「定向推送」信息（即利用個人信息和演算法推送個性化的新聞信息、商業廣告等），應當以明顯方式標明「定推」字樣，並提供停止接收定向推送信息的選項⁴¹。

38 《數據安全管理辦法》（徵求意見稿）第21條

39 《數據安全管理辦法》（徵求意見稿）第6及第19條

40 《數據安全管理辦法》（徵求意見稿）第35條

41 《數據安全管理辦法》（徵求意見稿）第23條

罰則

32. 網絡運營者違反《數據安全管理辦法》的規定，可被沒收違法所得（如有）、暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或營業執照⁴²。

(3) 《個人信息出境安全評估辦法》（徵求意見稿）⁴³

33. 《個人信息出境安全評估辦法》主要為落實《網絡安全法》下有關限制個人信息出境的規定，具法律約束力。



42 《數據安全管理辦法》（徵求意見稿）第37條

43 有關《個人信息出境安全評估辦法》的簡介是基於網信辦於2019年6月13日發布的徵求意見稿。截至2019年11月22日，《個人信息出境安全評估辦法》的正式版本仍未發布。

安全評估

34. 網絡運營者向境外提供在中國內地運營中收集的個人信息，應當按照此辦法進行安全評估。經安全評估認定個人信息出境可能影響國家安全、損害公共利益，或者難以有效保障個人信息安全的，不得出境⁴⁴。
35. 網絡運營者在完成安全評估後，須向省級網信部門申報，並提交網絡運營者與接收者簽訂的合同、個人信息出境安全風險及安全保障措施分析報告等資料。省級網信部門在收到相關文件後，應當在15個工作日內完成審核⁴⁵。網絡運營者在獲得省級網信部門的許可後方可將個人信息轉移至境外。

合同

36. 就個人信息出境的相關合同方面，網絡運營者須加入指定條款，包括：
 - (a) 個人信息出境的目的、類型、保存期限；
 - (b) 個人信息主體是合同中涉及個人信息主體權益的條款的受益人；
 - (c) 個人信息主體合法權益受到損害時，可以向網絡運營者及／或接收者索賠；
 - (d) 網絡運營者有責任應個人信息主體的要求提供合同副本⁴⁶。

44 《個人信息出境安全評估辦法》(徵求意見稿)第2條

45 《個人信息出境安全評估辦法》(徵求意見稿)第3至5條

46 《個人信息出境安全評估辦法》(徵求意見稿)第13條

監督執行

37. 網絡運營者應當在每年12月31日前將該年度個人信息出境情況、合同履行情況等向所在地省級網信部門報告⁴⁷。
38. 省級網信部門應定期檢查網絡運營者的個人信息出境情況，並重點檢查有關合同的履行情況、有否違反國家規定，以及有否損害個人信息主體合法權益等。若發現違規情況，可要求網絡運營者整改，甚至暫停或終止個人信息出境⁴⁸。

境外效力

39. 如果境外機構在經營活動中，通過互聯網等收集中國內地使用者的個人信息，有關機構應當在中國內地通過法定代表人或者機構履行《個人信息出境安全評估辦法》中網路運營者的責任和義務⁴⁹。換言之，《個人信息出境安全評估辦法》具境外效力。

47 《個人信息出境安全評估辦法》(徵求意見稿)第9條

48 《個人信息出境安全評估辦法》(徵求意見稿)第10條

49 《個人信息出境安全評估辦法》(徵求意見稿)第20條

(4) 《兒童個人信息網絡保護規定》

40. 《兒童個人信息網絡保護規定》是網信辦根據《網絡安全法》和《未成年人保護法》等法律制定，目的是為了保護兒童個人信息安全，促進兒童健康成長，並自2019年10月1日起施行⁵⁰。



41. 《兒童個人信息網絡保護規定》具法律約束力。在中國內地通過網絡從事收集、存儲、使用、轉移、披露兒童個人信息等活動須遵從此規定⁵¹。
42. 網絡運營者在處理兒童個人信息時除了要遵守《網絡安全法》及其相關規章中有關個人信息的通用規定外，還要特別留意《兒童個人信息網絡保護規定》中一些為保護兒童個人信息而設的額外規定。

50 《兒童個人信息網絡保護規定》第1及第29條

51 《兒童個人信息網絡保護規定》第3條

43. 根據《兒童個人信息網絡保護規定》，「兒童」的定義為未滿14周歲的未成年人⁵²。
44. 網絡運營者應當設置專門的兒童個人信息保護規則和用戶協議，並指定專人負責兒童個人信息保護⁵³。
45. 網絡運營者收集、使用、轉移、披露兒童個人信息時，應當以顯著、清晰的方式告知兒童監護人，並應當徵得兒童監護人的同意⁵⁴。
46. 兒童或其監護人有權就相關兒童的個人信息提出更正或刪除的要求⁵⁵。
47. 網絡運營者對其工作人員應當以最少授權為原則，嚴格設定兒童個人信息的查閱權限，並須在查閱前經過兒童個人信息保護負責人或者其授權的管理人員審批，記錄查閱情況，並採取技術措施避免違法複製、下載兒童個人信息⁵⁶。
48. 網絡運營者向第三方轉移兒童個人信息前，應當自行或者委託第三方機構進行安全評估⁵⁷。
49. 網絡運營者如違反《兒童個人信息網絡保護規定》，網信辦或其他相關部門可根據《網路安全法》等相關法規的規定處理。如構成犯罪的，可依法追究刑事責任⁵⁸。

52 《兒童個人信息網絡保護規定》第2條

53 《兒童個人信息網絡保護規定》第8條

54 《兒童個人信息網絡保護規定》第9條

55 《兒童個人信息網絡保護規定》第19及20條

56 《兒童個人信息網絡保護規定》第15條

57 《兒童個人信息網絡保護規定》第17條

58 《兒童個人信息網絡保護規定》第26條

(5) 《個人信息安全規範》(徵求意見稿)⁵⁹

50. 《個人信息安全規範》由國家標準化管理委員會及國家質量監督檢驗檢疫總局聯合發布，作為個人信息保護實務措施的國家標準及良好行事方式指引，規範「個人信息控制者」在收集、保存、使用、共用、轉讓、公開披露等信息處理環節中的相關行為，其準則與目前國際普遍認可的個人信息保護標準(例如經濟合作與發展組織的《私隱指引》和歐盟的《通用數據保障條例》)相近。
51. 《個人信息安全規範》本身不具法律約束力，然而違反當中的指引有可能被執法機關視作違反個人信息保護法規的相關規定。因此，各機構在遵從《消費者權益保護法》、《網絡安全法》、《數據安全管理辦法》等法規中有關個人信息的規定同時，亦應參考《個人信息安全規範》中的指引。



59 《個人信息安全規範》的第一版於2017年12月29日發布，並於2018年5月1日實施。在2019年，國家標準化管理委員會及國家質量監督檢驗檢疫總局聯合推出了第二版的《個人信息安全規範》的徵求意見稿，最新版本的徵求意見稿的發布日期為2019年10月24日。截至2019年11月22日，第二版的《個人信息安全規範》的正式版本仍未發布。以上有關《個人信息安全規範》的簡介是基於新版本的徵求意見稿製作。

定義

52. 《個人信息安全規範》為「個人信息」、「個人敏感信息」、「個人信息控制者」、「授權同意」和「明示同意」等概念作出定義。
53. 「個人信息」是指「以電子或者其他方式記錄的能夠單獨或者與其他信息結合識別特定自然人身份或者反映特定自然人活動情況的各種信息⁶⁰。」此定義與最高人民法院及最高人民檢察院的聯合解釋相似，並比《網絡安全法》下的定義更廣。
54. 「個人敏感信息」則指「一旦洩露、非法提供或濫用可能危害人身和財產安全，極易導致個人名譽、身心健康受到損害或歧視性待遇等的個人信息」，具體例子包括身份證件號碼、個人生物識別信息、銀行帳號、通信記錄和內容、財產信息、徵信信息、行蹤軌跡、住宿信息、健康生理信息、交易信息以及14歲以下兒童的個人信息等⁶¹。
55. 「個人信息控制者」的定義為「有權決定個人信息處理目的、方式等的組織或個人⁶²」，與世界其他地區的個人信息保護法的定義相近，不只限於「網絡運營者」。因此《個人信息安全規範》的適用範圍比《網絡安全法》、《消費者權益保護法》等法規更廣。

60 《個人信息安全規範》(徵求意見稿)第3.1段

61 《個人信息安全規範》(徵求意見稿)第3.2段

62 《個人信息安全規範》(徵求意見稿)第3.4段

個人信息安全基本原則

56. 《個人信息安全規範》確立了七項與國際標準接軌的個人信息安全基本原則，即(1)權責一致原則、(2)目的明確原則、(3)選擇同意原則、(4)最少夠用原則、(5)公開透明原則、(6)確保安全原則、(7)主體參與原則⁶³。

權責一致原則(問責制)

57. 就「權責一致原則」方面，《個人信息安全規範》要求個人信息控制者採取技術和其他必要的措施保障個人信息的安全，並對個人信息主體合法權益造成的損害承擔責任。此外，《個人信息安全規範》亦要求符合有關門檻⁶⁴的個人信息控制者任命專職的個人信息保護負責人和設立個人信息保護工作機構，負責個人信息安全工作⁶⁵。個人信息控制者亦應建立個人信息安全影響評估制度，評估並處置個人信息處理活動存在的安全風險⁶⁶。若發生個人信息安全事故，個人信息控制者應通知個人信息主體，並向其提供補救措施⁶⁷。

63 《個人信息安全規範》(徵求意見稿)第4段—個人信息安全基本原則：

- (1) 權責一致原則—採取技術和其他必要的措施保障個人信息的安全，對其個人信息處理活動對個人信息主體合法權益造成的損害承擔責任。
- (2) 目的明確原則—具有合法、正當、必要、明確的個人信息處理目的。
- (3) 選擇同意原則—向個人信息主體明示個人信息處理目的、方式、範圍、規則等，徵求其授權同意。
- (4) 最少夠用原則—只處理滿足個人信息主體授權同意的目的所需的最少個人信息類型和數量。目的達成後，應及時刪除個人信息。
- (5) 公開透明原則—以明確、易懂和合理的方式公開處理個人信息的範圍、目的、規則等，並接受外部監督。
- (6) 確保安全原則—具備與所面臨的安全風險相匹配的安全能力，並採取足夠的管理措施和技術手段，保護個人信息的保密性、完整性、可用性。
- (7) 主體參與原則—向個人信息主體提供能夠查詢、更正、刪除其個人信息，以及撤回授權同意、註銷帳戶、投訴等方法。

64 有關門檻為(1)主要業務涉及個人信息處理，且從業人員規模大於200人，或(2)處理超過100萬人的個人信息，或預計在12個月內處理超過100萬人的個人信息。詳見《個人信息安全規範》(徵求意見稿)第10.1(c)段。

65 《個人信息安全規範》(徵求意見稿)第10.1段

66 《個人信息安全規範》(徵求意見稿)第10.4段

67 《個人信息安全規範》(徵求意見稿)第9.2段

授權同意與明示同意

58. 《個人信息安全規範》要求個人信息控制者在收集個人信息時要告知個人信息主體收集、使用個人信息的目的、方式和範圍，獲得其「授權同意」（除非是例外情況⁶⁸），並且不應通過捆綁產品或服務各項業務功能的方式，要求個人信息主體一次性接受並授權同意各項業務功能收集個人信息的請求⁶⁹。「授權同意」是指個人信息主體作出的明確授權行為，當中包括通過積極的行為（即「明示同意」；見下文）以及消極的不作為所作出的授權（例如，個人信息主體獲告知會被收集個人信息後並沒有選擇離開有關信息採集區域⁷⁰）。
59. 如果個人信息控制者所收集的信息屬個人敏感信息⁷¹，或者因業務需要而確需將個人信息用於超出收集時所表述的目的或其合理關聯範圍⁷²，便應向個人信息主體取得「明示同意」。「明示同意」即個人信息主體要通過書面、口頭等方式主動聲明或自主作出肯定性動作以表達同意，例如主動勾選、主動點擊「同意」、主動填寫或提供等。

自動決策

60. 如果個人信息控制者的信息系統具備自動決策機制，且能對個人信息主體權益造成顯著影響（例如自動決定個人徵信及貸款額度，或用於面試人員的自動化篩選等），個人信息控制者應該在規劃設計階段，以及在使用過程中定期開展個人信息安全影響評估及依評估結果採取有效的保護措施，並且向個人信息主體提供針對自動決策結果的申訴管道⁷³。

68 例外情況包括為履行法律責任、履行與個人信息主體簽訂的合同，以及為國家安全、重大公眾利益及偵查罪案等。詳見《個人信息安全規範》第5.6段。

69 《個人信息安全規範》（徵求意見稿）第5.3及5.4段

70 《個人信息安全規範》（徵求意見稿）第3.7段

71 《個人信息安全規範》（徵求意見稿）第5.4(b)段

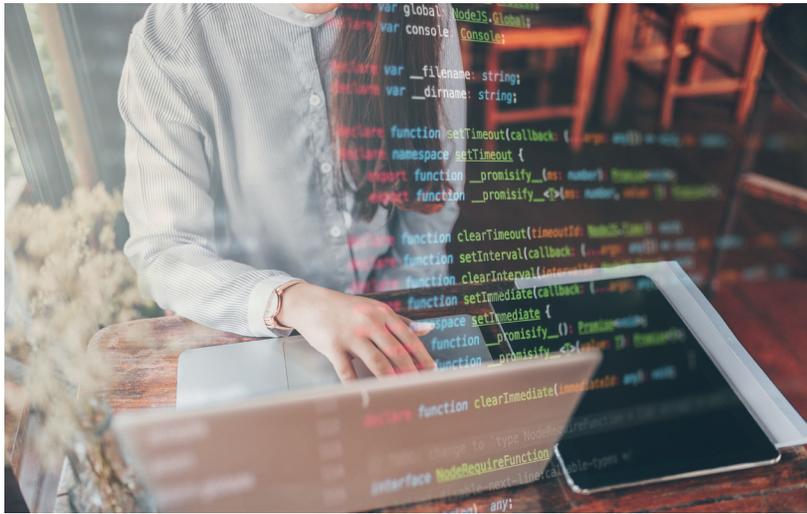
72 《個人信息安全規範》（徵求意見稿）第7.3段

73 《個人信息安全規範》（徵求意見稿）第7.7段

主體參與

61. 至於「主體參與原則」方面，個人信息控制者須向個人信息主體提供能夠查詢、更正、刪除其個人信息，以及撤回授權同意、注銷帳戶、投訴等方法⁷⁴。

(6) 《網絡安全威脅信息發布管理辦法》(徵求意見稿)⁷⁵



62. 為規管網絡安全威脅信息的發布行為，網信辦及公安部等有關部門依據《網絡安全法》，聯合草擬了《網絡安全威脅信息發布管理辦法》。「網絡安全威脅信息」包括與電腦病毒、網絡攻擊、網絡侵入、網絡安全事件、系統漏洞等有關的信息⁷⁶。管理辦法列明，發布網絡安全威脅信息的目的是維護和促進網絡安全，並且不得危害國家安全及公眾利益，亦不得侵犯公民及其他組織的合法權益⁷⁷。信息發布者不得利用網絡安全威脅信息進行炒作、牟取不正當利益或從事不正當商業競爭⁷⁸。

74 《個人信息安全規範》(徵求意見稿)第7.8-7.15段

75 有關《網絡安全威脅信息發布管理辦法》的簡介是基於網信辦於2019年11月20日發布的徵求意見稿。截至2019年11月22日，《網絡安全威脅信息發布管理辦法》的正式版本仍未發布。

76 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第12條

77 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第2條

78 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第3條

63. 任何企業、組織或個人在發布網絡安全威脅信息前，應事先向相關網信部門及公安機關報告。若有關網絡安全威脅信息涉及公共通信和信息服務、能源、交通、水利、金融、公共服務、電子政務、國防科技工業等重要行業和領域，發布者亦應事先向行業主管部門報告⁷⁹。
64. 任何企業、組織或個人在發布具體網絡和信息系統存在風險、脆弱性情況前，應事先徵求網絡和信息系統運營者書面意見，除非（1）相關風險、脆弱性已被消除或修復，或（2）在發布前30日已向網信、電信、公安或相關行業主管部門舉報⁸⁰。
65. 管理辦法亦列明，發布的網絡安全威脅信息不得包含某些指定信息，例如惡意程式的源代碼和製作方法、能夠完整復現網絡攻擊的細節信息、數據外洩事件中所洩露的數據等⁸¹。
66. 傳媒機構及其他人士不得利用大眾媒體、社交網絡、講座等途徑傳播在違反此管理辦法下發布的網絡安全威脅信息⁸²。
67. 任何企業、組織或個人違反此管理辦法，將由網信部門、公安機關按《網絡安全法》的規定處理⁸³。

79 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第5至6條

80 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第8條

81 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第4條

82 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第9條

83 《網絡安全威脅信息發布管理辦法》(徵求意見稿)第10條

(七) 《電子商務法》

68. 自 2019 年 1 月 1 日起實施的《電子商務法》主要規管在中國內地通過互聯網等信息網絡銷售商品或提供服務的行業。其立法目的為保障電子商務各方主體的合法權益、規範電子商務行為、維護市場秩序，以及促進電子商務持續健康發展⁸⁴。
69. 電子商務經營者從事經營活動時，須履行消費者權益保護、網絡安全以及個人信息保護等方面的義務⁸⁵，當中包括：遵守法律、行政法規中有關收集、使用個人信息的規定⁸⁶；向用戶明示有關用戶信息查詢、更正、刪除及注銷帳戶等的方式，並且不得就用戶的上述要求設置不合理條件⁸⁷。
70. 如果電子商務經營者根據消費者的興趣愛好、消費習慣等特徵向其提供商品或者服務的搜尋結果(即個性化推薦)，應當同時向該消費者提供關閉個性化推薦的功能的選擇，尊重和平等保護消費者合法權益⁸⁸。
71. 電子商務平台經營者應當採取技術措施和其他必要措施保證其網絡安全、穩定運行，並制定網絡安全事件應急預案。在發生網絡安全事件時，應當立即啟動應急預案，採取相應的補救措施，並向有關主管部門報告⁸⁹。
72. 電子商務平台經營者應當記錄、保存平台上的交易信息，並確保信息的完整性、保密性、可用性。保存時間為自交易完成之日起不少於三年⁹⁰。
73. 電子商務平台經營者如違反上述規定，視乎嚴重程度，可被有關主管部門(例如市場監督管理部門)責令限期改正及處以最高 50 萬元罰款，甚或被責令停業整頓及罰款；如涉及保護個人信息的規定，亦可依照《網路安全法》等法律、行政法規的規定處罰⁹¹。

84 《電子商務法》第 1 至 2 條

85 《電子商務法》第 5 條

86 《電子商務法》第 23 條

87 《電子商務法》第 24 條

88 《電子商務法》第 18 條

89 《電子商務法》第 30 條

90 《電子商務法》第 31 條

91 《電子商務法》第 76(3)、79 及 80(4) 條

(八) 其他行政法規、部門規章和指引

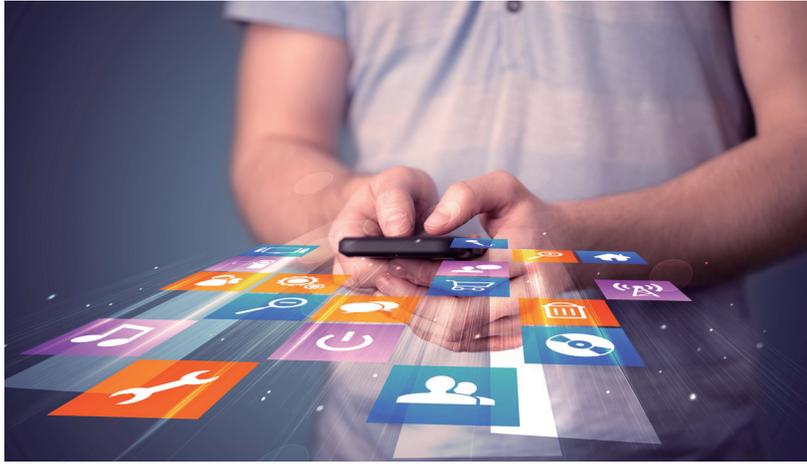
74. 除了上述的法規，中國內地不同的政府部門及監管機構亦有就個別行業或活動的需要而制定了相關的個人信息保護規定或指引。由於數目眾多，以下只摘錄一些例子以供參考。各機構如在內地進行個人信息收集、處理、使用等活動，應該諮詢專業法律意見，以確保符規。

(1) 《銀行業金融機構數據治理指引》

75. 中國銀行保險監督管理委員會根據《銀行業監督管理法》等法規，於2018年5月21日發布了此指引，藉此明確銀行和金融機構的數據治理架構，提高業界的數據管理和數據質量。



(2) 《移動互聯網應用程式信息服務管理規定》



76. 為加強對移動互聯網應用程式信息服務的規範管理，建立健全使用者信息安全保護機制，懲治侵犯公民個人信息犯罪活動，網信辦於2016年8月1日起實施了《移動互聯網應用程式信息服務管理規定》，規管互聯網應用程式提供者的責任和義務，保障使用者在安裝及使用程式時的知情權及選擇權，以及保護及尊重知識財產權。

(3) 《移動互聯網應用(App)收集個人信息基本規範》(草案)⁹²

77. 為落實《網絡安全法》對個人信息保護的相關要求，加快相應標準化工作，國家標準化管理委員會及國家市場監督管理總局聯合發布了此草案，明確了移動互聯網應用程式收集個人信息時應滿足的基本要求，當中包括列明哪些信息及許可權對互聯網應用程式的正常運作屬必須，並建議互聯網應用程式的運營者不應因使用者拒絕提供非必要的信息或許可權而拒絕提供服務。



92 有關《移動互聯網應用(App)收集個人信息基本規範》的簡介是基於國家標準化管理委員會及國家市場監督管理總局於2019年10月25日聯合發布的草案。截至2019年11月22日，《移動互聯網應用(App)收集個人信息基本規範》的正式版本仍未發布。



結語



(九) 結語

78. 在中國內地，涉及個人信息保護的法規數目眾多，並且隨著網絡信息技術和數字經濟的快速發展而不斷推陳出新，以加強個人信息保護，因此本簡介並未涵蓋所有相關的法規。就個別提述到的法規，本簡介亦未能詳細列出當中所有相關規定。各機構如在內地進行個人信息收集、處理、使用等活動，應該諮詢專業法律意見，以確保符規。
79. 從總體上看，中國內地的個人信息保護仍呈現分散立法狀態。值得注意的是，第十三屆全國人民代表大會常務委員會(任期為2018年3月至2023年3月)已將制定個人信息保護法列入本屆立法規劃。換言之，中國內地在不久將來應該會有一套全面的個人信息保護法。

附錄 1 — 內地有關個人信息保障法規的訂立時間表

名稱	訂立／發布日期	實施日期	連結
《侵權責任法》	2009年12月26日	2010年7月1日	http://www.gov.cn/fffg/2009-12/26/content_1497435.htm
《消費者權益保護法》第二次修正	2013年10月25日	2014年3月15日	http://www.gov.cn/jrzg/2013-10/25/content_2515601.htm
《刑法修正案(九)》	2015年8月29日	2015年11月1日	https://www.spp.gov.cn/spp/fl/201802/t20180205_364562.shtml
《移動互聯網應用程序信息服務管理規定》	2016年06月28日	2016年8月1日	http://www.cac.gov.cn/2016-06/28/c_1119123114.htm
《網絡安全法》	2016年11月7日	2017年6月1日	http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm
《民法總則》	2017年3月15日	2017年10月1日	http://www.gov.cn/xinwen/2017-03/18/content_5178585.htm#1
《最高人民法院最高人民檢察院關於辦理侵犯公民個人信息刑事案件適用法律若干問題的解釋》	2017年5月8日	2017年6月1日	https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml
《銀行業金融機構數據治理指引》	2018年5月21日	2018年5月21日	http://www.gov.cn/xinwen/2018-05/23/content_5292938.htm

名稱	訂立／發布日期	實施日期	連結
《電子商務法》	2018年8月31日	2019年1月1日	http://www.gov.cn/xinwen/2018-08/31/content_5318220.htm
《兒童個人信息網絡保護規定》	2019年8月22日	2019年10月1日	http://www.gov.cn/xinwen/2019-08/23/content_5423865.htm
《數據安全管理辦法》	2019年5月28日 (徵求意見稿)	尚未實施	http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm
《個人信息出境安全評估辦法》	2019年6月13日 (徵求意見稿)	尚未實施	https://www.cac.gov.cn/2019-06/13/c_1124613618.htm
《個人信息安全規範》	第一版： 2017年12月29日 第二版： 2019年10月24日 (徵求意見稿)	第一版： 2018年5月1日 第二版： 尚未實施	http://pip.tc260.org.cn/jbxt/privacy/detail/201910232235364993
《移動互聯網應用(App)收集個人信息基本規範》	2019年10月25日 (草案)	尚未實施	http://pip.tc260.org.cn/jbxt/privacy/detail/2019102501284491099
《民法典人格權編》	2019年8月28日 (草案三次審議稿)	尚未實施	(人大網) http://www.npc.gov.cn/npc/cw36/201908/70b9b2fa5b72475dda54ec33121d4bf.shtml (東方法眼網) http://www.dffyw.com/fazhixinwen/lifa/201908/46517.html
《網絡安全威脅信息發布管理辦法》	2019年11月20日 (徵求意見稿)	尚未實施	http://www.cac.gov.cn/2019-11/20/c_1575785387932969.htm

附錄 2 — 內地個人信息保障法規簡覽

	收集	使用及披露	透明度	保安	保存期限	問責制	外洩通報	跨境數據轉移	個性化及自動決策	查閱及更正權	刪除權
《網路安全法》	第 41 條	第 41、42 條	第 41 條	第 40、42 條		第 40 條	第 42 條	第 37 條		第 43 條	第 43 條
《消費者權益保障法》	第 29 條	第 29 條	第 29 條	第 29 條							
《電子商務法》				第 30、31 條	第 24 條		第 30 條		第 18 條	第 24、53 條	第 24 條
《數據安全管理辦法》(徵求意見稿)(2019年5月)	第 11-13 條	第 22、27 條	第 7-9 條	第 19 條	第 20 條	第 17、18 條	第 35 條	第 28 條	第 23 條	第 21 條	第 21 條
《兒童個人信息網絡保護規定》	第 7、9、11 條	第 7、9、14 條	第 8、10 條	第 13、15 條	第 12、23 條	第 8 條	第 21 條			第 19 條	第 20 條
《個人信息出境安全評估辦法》(徵求意見稿)(2019年6月)							第 9 條	大部份條文			
《個人信息安全規範》(徵求意見稿)(2019年10月)	第 5.1-5.4 段	第 7.3 段	第 5.5 段	第 7.1、7.2、10.5 段	第 6.1、6.2、6.4、7.12 段	第 10 段	第 9.1、9.2 段	第 8.8 段	第 7.5、7.7 段	第 7.8、7.9 段	第 7.10、7.12 段

■ 具法律效力的規定(橙色的條文為個人信息保障作出較為細緻的規定)

■ 不具法律效力的建議良好行事方式

附錄3 — 香港《個人資料(私隱)條例》(《條例》)與內地保障個人信息相關法規的比較

	《個人資料(私隱)條例》	內地相關法規
立法目的	在個人資料方面保障個人的私隱。	視乎不同法規而定。 例如《網絡安全法》的主要目的為保障網絡、國家及社會安全，維護公民、法人和其他組織的合法權益，促進經濟社會信息化健康發展。《數據安全管理辦法》(徵求意見稿)的目的包括保障個人信息和重要數據安全。
規管對象	資料使用者，即就個人資料而言，獨自或聯同其他人或與其他人共同控制該資料的收集、持有、處理或使用的人。	視乎不同法規而定。 例如《網絡安全法》、《數據安全管理辦法》(徵求意見稿)和《兒童個人信息網絡保護規定》規管網絡運營者，《電子商務法》規管電子商務經營者，《消費者權益保護法》規管向消費者提供商品和服務的經營者。
個人資料／個人信息的定義	個人資料是指(1)直接或間接與一名在世的個人有關的任何資料，(2)而從該資料直接或間接地確定有關的個人的身分是切實可行，以及(3)該資料的存在形式必須是令查閱及處理均是切實可行的。	按《網絡安全法》，個人信息是指以電子或者其他方式記錄的能夠單獨或者與其他信息結合識別自然人個人身份的一種信息。 按最高人民法院及最高人民檢察院聯合公布的解釋，以及《個人信息安全規範》(徵求意見稿)，個人信息還包括可反映特定自然人活動情況的各種信息。

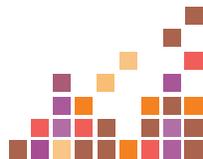
	《個人資料(私隱)條例》	內地相關法規
個人敏感信息	<p>《條例》沒有專屬定義。</p> <p>然而，《條例》附表1的保障資料第4原則的某些規定，可應用於保障個人敏感信息。該原則規定，資料使用者在個人資料保安方面，除了其他事宜外，尤其須考慮資料的種類，及因未獲准許的或意外的查閱、處理、刪除、喪失或使用而做成的損害。</p>	<p>按《個人信息安全規範》(徵求意見稿)，個人敏感信息是指一旦洩露、非法提供或濫用可能危害人身和財產安全，極易導致個人名譽、身心健康受到損害或歧視性待遇等的個人信息，具體例子包括身份證件號碼、個人生物識別信息、銀行帳號、通信記錄和內容、財產信息、微信信息、行蹤軌跡、住宿信息、健康生理信息、交易信息以及14歲以下兒童的個人信息等。</p> <p>《數據安全管理辦法》(徵求意見稿)要求收集敏感個人信息的網絡運營者向所在地的網信部門備案，並須明確數據安全責任人。</p>
收集	<p>《條例》附表1的保障資料第1原則規定，資料使用者須以合法和公平的方式收集他人的個人資料，收集目的須為合法目的並須是必需或直接與資料使用者的職能或活動有關，所收集的資料必須不超乎適度。</p>	<p>《網絡安全法》規定，收集、使用個人信息，應當遵循合法、正當、必要的原則，必須取得被收集者的同意。不得收集與提供的服務無關的個人信息。</p> <p>《數據安全管理辦法》(徵求意見稿)規定在收集個人信息時須向個人提供收集及使用個人信息的規則，並禁止以改善服務品質、提升用戶體驗、定向推送信息、研發新產品等為由，以預設授權、功能捆綁等形式強迫、誤導個人同意其收集個人信息。</p> <p>如收集的屬個人敏感信息，《數據安全管理辦法》(徵求意見稿)規定須向所在地的網信部門備案，而《個人信息安全規範》(徵求意見稿)則建議要取得個人的「明示同意」。</p> <p>《兒童個人信息網絡保護規定》要求收集和使用兒童個人信息前，須告知兒童的監護人，並取得監護人的同意。</p>

	《個人資料(私隱)條例》	內地相關法規
使用及披露	<p>《條例》附表1的保障資料第3原則規定，資料使用者使用(包括披露)個人資料的目的必須屬收集時的目的或直接有關的目的，否則須先取得資料當事人的訂明同意。</p>	<p>《網絡安全法》規定，收集、使用個人信息，應當遵循合法、正當、必要的原則，必須取得被收集者的同意。</p> <p>《數據安全管理辦法》(徵求意見稿)規定使用個人信息時，不得違反向個人說明了的收集、使用規則。如因業務需要，確需擴大個人信息使用範圍，須徵得個人同意。若要向第三方披露個人信息，須先評估安全風險，並取得個人同意。</p> <p>《兒童個人信息網絡保護規定》要求收集和使用兒童個人信息前，須告知兒童的監護人，並取得監護人的同意。</p>
透明度	<p>《條例》附表1的保障資料第1原則規定，資料使用者須採取所有切實可行的步驟，以確保在收集個人資料之時或之前，資料當事人獲告知收集其個人資料的目的、資料可能會被轉移給哪類人士、資料當事人是否有責任提供資料，及不提供資料的後果。</p> <p>《條例》附表1的保障資料第5原則規定，資料使用者須採取所有切實可行的步驟，以確保任何人能確定資料使用者在個人資料方面的政策及實務，並能獲告知資料使用者所持有的個人資料的種類及使用之主要目的。</p>	<p>《網絡安全法》及《數據安全管理辦法》(徵求意見稿)規定要公開收集、使用規則，明示收集、使用信息的目的、方式和範圍等。</p> <p>《兒童個人信息網絡保護規定》要求設置專門的兒童個人信息保護規則和用戶協議，有關規則和協議應當簡潔、易懂。</p>

	《個人資料(私隱)條例》	內地相關法規
保安	<p>《條例》附表 1 的保障資料第 4 原則規定 —</p> <ul style="list-style-type: none"> • 資料使用者須採取所有切實可行的步驟，以確保由其持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響。 • 如聘用資料處理者代為處理個人資料，資料使用者須採取合約規範方法或其他方法，以防止轉移予資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。 	<p>《網絡安全法》規定要採取技術措施和其他必要措施，確保其收集的個人信息安全，防止信息洩露、毀損、丟失。</p> <p>《數據安全管理辦法》(徵求意見稿)要求網絡運營者參照國家相關標準，建立數據安全管理制度，制定數據安全計劃，實施數據安全技術防護(例如數據分類、備份、加密等)以保障數據安全。</p>
保存期限	<p>《條例》附表 1 的保障資料第 2(2) 原則規定，資料使用者須採取所有切實可行的步驟，以確保個人資料的保存時間不超過為貫徹使用該資料之目的而所需的時間。</p> <p>《條例》第 26 條規定，資料使用者須採取所有切實可行步驟，刪除不再需要的個人資料。</p>	<p>按《數據安全管理辦法》(徵求意見稿)，個人信息保存期不應超出收集使用規則中的保存期限。</p> <p>《電子商務法》規定在用戶註銷帳戶後立即刪除有關用戶的信息。</p>

	《個人資料(私隱)條例》	內地相關法規
準確性	<p>《條例》附表1的保障資料第2(1)原則規定—</p> <ul style="list-style-type: none"> 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。 若有合理理由相信個人資料不準確時，資料使用者須確保該資料不會被使用或會被刪除。 若知悉向第三者披露的個人資料在要項上不準確時，資料使用者須確保第三者獲告知，及獲提供所需詳情以令第三者能更正。 	<p>《個人信息安全規範》(徵求意見稿)在「確保安全原則」下建議要採取措施保護個人信息的完整性和可用性。</p>
問責制	<p>《條例》沒有相關規定。</p> <p>個人資料私隱專員鼓勵資料使用者實行「私隱管理系統」以實踐問責制。</p>	<p>《網絡安全法》規定網絡運營者應當對其收集的個人信息嚴格保密，並建立健全的信息保護制度。</p> <p>《數據安全管理辦法》(徵求意見稿)明確要求開展數據安全風險評估，制定網絡安全事件應急預案，並組織數據安全教育、培訓。</p> <p>《兒童個人信息網絡保護規定》要求有指定專人負責兒童個人信息保護。</p> <p>《個人信息安全規範》(徵求意見稿)建議任命專職的個人信息保護負責人和設立個人信息保護工作機構，負責個人信息安全工作。</p>

	《個人資料(私隱)條例》	內地相關法規
外洩通報	<p>《條例》沒有相關規定。</p> <p>個人資料私隱專員鼓勵資料使用者發現個人資料外洩時通報受影響人士及相關規管／執法機構。</p>	<p>《網絡安全法》、《電子商務法》、《兒童個人信息網絡保護規定》、《數據安全管理辦法》(徵求意見稿)及《個人信息出境安全評估辦法》(徵求意見稿)均規定在發生或者可能發生個人信息洩露或其他信息安全事故時，應當立即向有關主管部門報告，甚或通知受影響的個人。</p> <p>《網絡安全威脅信息發布管理辦法》(徵求意見稿)規定，任何企業、組織或個人在發布網絡安全威脅信息前，應事先向相關網信部門及公安機關報告。</p>
跨境數據轉移	<p>《條例》第33條規管(1)在香港收集、持有、處理或使用的個人資料，或(2)主要業務地點在香港的資料使用者，控制收集、持有、處理或使用的個人資料。</p> <p>該條規定，除非符合《條例》下的指明條件(例如得到資料當事人的書面同意，或資料使用者已採取所有合理的預防措施及已作出所有應作出的努力，以對個人資料提供足夠的保護)，否則受規管的個人資料不得轉移離開香港。但相關規定尚未實施。</p>	<p>《網絡安全法》規定「關鍵信息基礎設施」的運營者須將個人信息及重要數據儲存在中國內地。如要出境，須進行安全評估。</p> <p>《個人信息出境安全評估辦法》(徵求意見稿)將《網絡安全法》下的個人信息出境限制擴展至所有網絡運營者，並要求將安全評估向省級網信部門申報及取得其批准後方可將個人信息傳送到境外。</p>



	《個人資料(私隱)條例》	內地相關法規
<p>個性化及自動決策</p>	<p>《條例》沒有就個性化及自動決策，特定給予相關定義及作出相關規定。</p> <p>然而，《條例》第30至32條規管「核對程序」，而有關程序可能會應用於個性化的操作。</p> <p>「核對程序」指符合以下全部四項準則的程序：</p> <ol style="list-style-type: none"> (1) 有關程序將兩套為不同目的而收集的個人資料加以核對； (2) 每一項比較涉及十個或以上資料當事人； (3) 比較並非以人手方法進行； (4) 核對資料的結果可即時或在將來用來對有關資料當事人採取不利行動。 <p>除非獲資料當事人或個人資料私隱專員同意，資料使用者不得進行「核對程序」。</p>	<p>《電子商務法》規定如果電子商務經營者向個人提供個性化的商品或服務的搜尋結果，須容許個人關閉此個性化推薦的功能。</p> <p>《數據安全管理辦法》(徵求意見稿)規定如網絡運營者向個人推送個性化的新聞信息、商業廣告等，應當以明顯方式標明「定推」字樣，並提供停止接收定向推送信息的選項。</p> <p>《個人信息安全規範》(徵求意見稿)建議在進行會對個人信息主體權益造成顯著影響的自動決策前，須開展個人信息安全影響評估，並且向個人信息主體提供針對自動決策結果的申訴管道。</p>

	《個人資料(私隱)條例》	內地相關法規
查閱及更正權	《條例》第18及22條，及附表1的保障資料第6原則訂明，資料當事人有權向資料使用者要求查閱個人資料，及要求改正不準確的個人資料。	<p>《網絡安全法》規定個人有權要求網絡運營者更正錯誤的個人信息。</p> <p>《數據安全管理辦法》(徵求意見稿)規定網絡運營者要遵從個人查閱及更正個人信息的要求。</p> <p>《電子商務法》規定電子支付服務提供者須向使用者免費提供最近三年的交易記錄。</p>
刪除權	<p>資料當事人沒有明確的權利要求刪除其個人資料。</p> <p>然而，《條例》第26條及附表1的保障資料第2(2)原則規定，資料使用者須採取所有切實可行步驟，刪除不再需要的個人資料。</p>	<p>按《網絡安全法》，如網絡運營者違規收集或使用個人信息，個人有權要求網路運營者將信息刪除。</p> <p>《數據安全管理辦法》(徵求意見稿)亦規定網絡運營者要在合理的代價和時間內遵從個人刪除個人信息的要求。</p>
執法機構	個人資料私隱專員	沒有單一、指定的執法機構。視乎行業和案件性質，執法機構可以為網信辦、公安部、工信部或其他主管部門。



	《個人資料(私隱)條例》	內地相關法規
罰則	<p>個人資料私隱專員可向違反《條例》的規定的資料使用者發出執行通知。不遵守執行通知是刑事罪行，違者如屬首次定罪，最高可判罰款港幣五萬元及監禁兩年；如屬再次定罪，最高可判罰款港幣十萬元及監禁兩年。</p> <p>違反《條例》的某些規定亦構成刑事罪行，違者可判罰款甚至監禁。例如(1)為得益而沒有依從資料當事人的要求，停止將該當事人的個人資料提供予其他人在直接促銷中使用，或(2)披露未經資料使用者同意而獲取的個人資料並導致有關資料當事人蒙受心理傷害，最高可判罰款港幣 100 萬元及監禁五年。</p>	<p>視乎不同法規而定。</p> <p>例如違反《網絡安全法》的規定可被責令改正，並根據情節嚴重程度而處以警告、沒收違法所得(如有)、處以罰款(最高為違法所得的十倍或人民幣 100 萬元)、對直接負責的主管人員和其他直接責任人員處以最高人民幣 10 萬元罰款，甚或責令暫停相關業務、停業整頓、關閉網站、吊銷相關業務許可證或營業執照。如構成犯罪的，依法追究刑事責任。</p>
民事索償	<p>根據《條例》第 66 條，資料當事人因資料使用者違反《條例》而蒙受損害(包括感情傷害)，有權向該資料使用者申索補償。</p> <p>根據《條例》第 66B 條，個人資料私隱專員可就申索補償的法律程序，向有關資料當事人給予協助，當中包括(1)提供意見、(2)安排律師或大律師提供意見或協助及(3)安排其他人代表該資料當事人行事。</p>	<p>根據《民法總則》，侵犯公民的隱私權或個人信息須要承擔民事責任，當中包括停止侵害、賠償損失、消除影響、恢復名譽及賠禮道歉。</p>

內地民商事務所涉

個人信息及網絡安全 主要法規簡介

目前中國內地針對個人信息保護方面的規管分散於多部法律、行政法規、部門規章和指引等規範性文件中，有關監管框架也在不斷擴張。此外，中國內地亦開始著重將隱私權及個人信息權視為獨立的人格權，並賦予民事保障。

隨著各種法規的出台，社會大眾的隱私和個人信息受到更廣泛及更大程度的保障。然而，由於中國內地關乎個人信息保護的法規眾多，期待到這個新興市場擴展業務的企業須面對符規方面的挑戰。本簡介旨在幫助各個與內地有聯繫或業務往來的機構、企業掌握有關內地法規，從而對推動粵港澳大灣區的發展作出微薄的貢獻，亦希望本簡介能成為創新科技企業的「工具箱」，幫助他們在發展和運用大數據、雲端計算、人工智能等技術時邁向成功。

香港個人資料私隱專員公署



www.pcpd.org.hk

下載本簡介



出版

香港個人資料私隱專員
香港灣仔皇后大道東248號陽光中心13樓1303室
網址：www.pcpd.org.hk
電郵：enquiry@pcpd.org.hk

Published by

Privacy Commissioner for Personal Data, Hong Kong
Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong
Website: www.pcpd.org.hk
E-mail: enquiry@pcpd.org.hk

版權

Copyright



本刊物使用署名4.0國際(CC BY 4.0)的授權條款，只要你註明原創者為香港個人資料私隱專員，便可自由分享或修改本刊物。詳情請瀏覽 creativecommons.org/licenses/by/4.0/deed.zh。
國際統一書號：978-962-86939-0-0

This publication is licensed under Attribution 4.0 International (CC By 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0
ISBN: 978-962-86939-0-0

This booklet is printed on environment friendly paper
本書刊採用環保紙印刷



ISBN 978-962-86939-0-0



9 789628 693900

Published and printed in Hong Kong