■ 資料來源：香港個人資料私隱專員公署

內地《個人信息保護法》重點內容

《個人信息保護法》（下稱：《保護法》）於2021年8月20日經全國人大常委會通過，將於同年11月1日起施行。這是內地首部針對個人信息保護而訂立的法律。《保護法》確立以個人的同意為處理個人信息的主要法律基礎，規定處理個人信息須遵循合法、正當、誠信、最少必要以及公開透明的原則，並且須具有明確、合理的目的。

個人有權向個人信息處理者（相當於香港《個人資料（私隱）條例》下的「資料使用者」）查閱、複製、更正以及要求刪除其個人信息，亦有權要求個人信息處理者提供轉移其個人信息至其他處理者的途徑。個人信息處理者在處理屬未滿十四周歲未成年人的個人信息時，須取得其父母或監護人的同意，及須制定專門的個人信息處理規則。

《保護法》禁止利用個人信息進行自動化決策以對個人在交易價格等交易條件上實施不合理的差別待遇（即俗稱「殺熟」行為）。此外，如果個人信息處理者通過自動化決策方式向個人進行信息推送或商業營銷，須向個人提供不針對其個人特徵的選項或便捷的拒絕方式。

個人信息處理者如要向境外提供個人信息，須取得個人的單獨同意，以及符合特定條件，例如通過國家網信部門組織的安全評估、取得規定的認證、或簽定國家網信部門制定的標準合同等。《保護法》具境外效力。境外機構如為向境內自然人提供產品或者服務，或者為分析、評估境內自然人的行為等而處理境內自然人的個人信息，亦須遵守《保護法》規定，及在境內設立專門機構或代表。

國家網信部門將負責統籌協調個人信息保護工作和相關監督管理工作。國務院有關部門亦會在各自職責範圍內負責個人信息保護和監督管理工作。

違反《保護法》規定的個人信息處理者，最高可被罰款人民幣五千萬元，或上一年度營業額的百份之五，並可被責令停業整頓、吊銷相關業務許可或營業執照等。

《個人信息保護法》內容重點

以下是香港個人資料私隱專員公署介紹《個人信息保護法》的重點內容，所載的資訊只作一般參考用途，並非為《保護法》的應用提供詳盡指引，亦不構成法律或其他專業意見。個人資料私隱專員並沒有就所載資訊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。個別機構或人士為符合《保護法》的規定，應尋求專業的法律意見。

1. 立法目的

保護個人信息權益、規範個人信息處理活動及促進個人信息的合理利用（《保護法》第一條）。

2. 規管對象

《保護法》規管在境內處理自然人個人信息的活動（《保護法》第三條），包括國家機關處理個人信息的活動（《保護法》第三十三條）。

個人信息處理者是指自主決定處理目的、處理方式等個人信息處理事項的組織、個人（《保護法》七十三條（一））。

3. 境外效力

境外機構如為向境內自然人提供產品或者服務，或者為分析、評估境內自然人的行為等，在境外進行個人信息處理活動，亦適用《保護法》（《保護法》第三條）。

符合《保護法》第三條第二款規定的境外個人信息處理者，應當在境內設立專門機構或者指定代表，負責處理個人信息保護相關事務（《保護法》第五十三條）。

4. 個人信息的定義

個人信息是以電子或者其他方式記錄，並**與已識別或者可識別的自然人有關**的各種信息，但不包括匿名化處理後的信息（《保護法》第四條）。

5. 敏感個人信息

敏感個人信息是指一旦洩露或者非法使用，容易導致自然人的人格尊嚴受到侵害或者人身、財產安全受到嚴重危害的個人信息，包括：生物識別、宗教信仰、特定身份、醫療健康、金融賬戶、行蹤軌跡等信息，以及未滿十四周歲未成年人的個人信息（《保護法》第二十八條）。

個人信息處理者須在具有特定的目的和充分的必要性，並採取嚴格保護措施的情況下，方可處理敏感個人信息（《保護法》第二十八條）。

處理敏感個人信息應當取得個人的單獨同意，除非法律、行政法規另有規定（《保護法》第二十九條）。

在公共場所安裝圖像採集、個人身份識別設備，應當為維護公共安全所必需，並設置顯著的提示標識。所收集的個人圖像、身份識別信息只能用於維護公共安全的目的，不得用於其他目的，除非取得個人單獨同意（《保護法》第二十六條）。

個人信息處理者應當在處理敏感個人信息前，進行個人信息保護影響評估，並將有關報告和記錄保存至少三年（《保護法》第五十五條至五十六條）。

6. 透明度

處理個人信息應當遵循公開、透明的原則，公開個人信息處理規則，明示處理目的、方式和範圍（《保護法》第七條）。

個人信息處理者在處理個人信息前，應當以**顯著**方式、**清晰易懂**的語言真實、準確、完整地向個人告知（1）其名稱或者姓名和聯繫方式；（2）處理目的、方式、個人信息種類及保存期限；以及（3）個人行使權利的方式和程序等事項（《保護法》第十七條）。

個人信息處理者如透過制定個人信息處理規則的方式提供上述資料，處理規則應當公開，而且便於查閱和保存（《保護法》第十七條）。

個人信息處理者如因合併、分立、解散、被宣告破產等原因需要轉移個人信息，應當向個人告知接收方的名稱或者姓名和聯繫方式（《保護法》第二十二條）。

7. 收集、使用及披露等

個人信息的處理是指包括個人信息的收集、存儲、使用、加工、傳輸、提供、公開、刪除等（《保護法》第四條）。

處理個人信息應當遵循**合法**、**正當**、**必要**和**誠信**原則，不得通過欺詐、誤導、脅迫等方式（《保護法》第五條）。

處理個人信息應當具有**明確**、**合理的目的**，並限於與處理目的直接相關，以及採取對個人權益影響最小的方式。收集個人信息應當限於實現處理目的的最小範圍，不得過度（《保護法》第六條）。

個人信息處理者只可在《個人信息保護法》列明的情況下處理個人信息，包括（1）取得個人的**同意**；（2）**為訂立、履行合同，或者為實施人力資源管理**；（3）**為履行法定職責／義務**；（4）**為公共利益進行新聞報道**；及（5）在合理的範圍內**處理個人自行公開或者其他已經合法公開的個人信息**（《保護法》第十三條）。

個人信息處理者如處理**未滿十四周歲未成年人**的個人信息，應當制定專門的個人信息處理規則（《保護法》第三十一條）。

任何組織、個人不得非法收集、使用、加工、傳輸、買賣、提供或公開他人的個人信息，以及不得從事危害國家安全、公共利益的個人信息處理活動（《保護法》第十條）。

8. 同意

個人的同意是指由個人在**充分知情**的前提下，**自願**、**明確**作出意思表示。法規規定應當取得個人單獨同意或者書面同意的，從其規定（《保護法》第十四條）。取得個人的同意是其中一個合法處理個人信息的情況（《保護法》第十三條）。

當處理目的、方式和個人信息種類有變更，應當重新取得個人同意（《保護法》第十四條）。

如果個人信息處理者處理已公開的個人信息會對個人權益有重大影響，應當取得個人同意（《保護法》第二十七條）

個人信息處理者於特定情況下須取得個人的**單獨同意**，包括：

- 向其他個人信息處理者提供其處理的個人信息（《保護法》第二十三條）；
- 公開其處理的個人信息（《保護法》第二十五條）；
- 處理敏感個人信息（《保護法》第二十九條）；
- 把在公共場所收集的個人圖像、身份識別信息用於維護公共安全以外的其他目的（《保護法》第二十六條）；及
- 向境外提供個人信息（《保護法》第三十九條）。

個人信息如屬未滿14周歲的未成年人，個人信息處理者應當取得其父母或監護人的同意（《保護法》第三十一條）。

個人信息處理者不得以個人不同意處理或撤回同意為由，拒絕提供產品或者服務（《保護法》第十六條）。

9. 保安

個人信息處理者應當對其個人信息處理活動負責，並**採取必要措施**保障所處理的個人信息的安全（《保護法》第九條）。

個人信息處理者如**委託第三方**處理個人信息，應當與受託人約定委託處理的目的、期限、方式、個人信息的種類、保護措施以及雙方的權利和義務等，並對受託人的個人信息處理活動進行監督（《保護法》第二十一條）。

接受委託處理個人信息的受託人，亦應當採取必要措施保障所處理的個人信息的安全（《保護法》第五十九條）。

10. 保存期限

個人信息的保存期限應當**為實現處理目的所必要的最短時間**（《保護法》第十九條）。

個人信息處理者應當在《個人信息保護法》列明的情況下主動或者根據個人的請求刪除個人信息，例如（1）當保存期限已屆滿、（2）處理目的已實現、無法實現或為實現處理目的不再必要、（3）個人撤回同意；或（4）個人信息處理者停止提供產品或服務等（《保護法》第四十七條）。

11. 準確性

處理個人信息應當保證個人信息的質量，避免因個人信息不準確、不完整對個人權益造成不利影響（《保護法》第八條）。

12. 問責與管治

個人信息處理者應當根據個人信息的處理目的、方式、個人信息的種類以及對個人**權益**的影響、可能存在的安全風險等，**採取下述措施確保個人信息處理活動符合法規**，並防止未經授權的訪問以及個人信息洩露、篡改、丟失，**措施包括**：（1）制定內部管理制度和操作規程；（2）對個人信息實行分類管理；以及（3）採取加密和去標識化安全技術措施（《保護法》第五十一條）。

處理個人信息達到國家網信部門規定數量的個人信息處理者應當指定**個人信息保護負責人**，負責對個人信息處理活動以及採取的保護措施等進行監督（《保護法》第五十二條）。

個人信息處理者應當定期對其處理個人信息遵守法律、行政法規的情況進行合規審計（《保護法》第五十四條）。

個人信息處理者應當在下列情況進行個人信息保護影響評估：（1）處理敏感個人信息；（2）利用個人信息進行自動化決策；（3）委託他人處理個人信息、向其他個人信息處理者提供或公開個人信息；（4）向境外提供個人信息；或（5）進行對個人權益有重大影響的個人信息處理活動。有關評估報告和記錄須保存至少三年（《保護法》第五十五條至五十六條）。

13. 互聯網平台的義務

提供重要互聯網平台服務、用戶數量巨大、業務類型複雜的個人信息處理者，應當履行特定義務，包括（1）建立健全個人信息保護合規制度體系，成立主要由外部成員組成的獨立機構，對個人信息處理活動進行監督；（2）遵循公開、公平、公正的原則，制定平台規則，明確平台內產品或者服務提供者處理個人信息的規範和保護個人信息的義務；（3）對嚴重違反法律、行政法規處理個人信息的平台內的產品或者服務提供者，停止提供服務；以及（4）定期發佈個人信息保護社會責任報告，接受社會監督（《保護法》第五十八條）。

14. 外洩通報

當發生或可能發生個人信息洩露、篡改、丟失時，個人信息處理者應當立即採取補救措施，並通知履行個人信息保護職責的部門和個人，通知應當包括（1）涉事的信息種類、事故原因和可能造成的危害；及（2）個人信息處理者已採取的補救措施和個人可以採取的減輕危害的措施等（《保護法》第五十七條）。

個人信息處理者如認為採取的措施能夠有效避免信息洩露、篡改、丟失造成的危害，可以不通知個人。但履行個人信息保護職責的部門如認為個人信息洩露可能對個人造成危害，有權要求個人信息處理者通知個人（《保護法》第五十七條）。

15. 跨境資料轉移

個人信息處理者如因業務等需要而需向境外提供個人信息，應當取得個人的**單獨同意**，並且具備下列一項條件（《保護法》第三十八條至三十九條）：

- 通過國家網信部門組織的安全評估；
- 按照國家網信部門的規定經專業機構進行個人信息保護認證；
- 按照國家網信部門制定的標準合同與境外接收方訂立合同，約定雙方的權利和義務；
- 法律、行政法規或者國家網信部門規定的其他條件。

如國家締結或者參加的國際條約、協定對境外提供個人信息的條件等有規定，可以按照其規定執行（《保護法》第三十八條）。

個人信息處理者應當採取必要措施，保障境外接收方處理個人信息的活動達到《個人信息保護法》規定的個人信息保護標準（《保護法》第三十八條）。

此外，個人信息處理者亦應當向個人**告知**境外接收方的名稱或者姓名、聯繫方式、處理目的、方式、個人信息的種類以及個人行使《保護法》規定權利的方式和程序等事項（《保護法》第三十九條）。

關鍵信息基礎設施運營者和處理**個人信息達到國家網信部門規定數量**的個人信息處理者，應當將在境內收集和產生的個人信息**儲存在境內**。如確需向境外提供，應當通過國家網信部門組織的安全評估，除非法規或國家網信部門另有規定可以不進行安全評估（《保護法》第四十條）。

16. 個性化及自動決策

自動化決策是指通過計算機程序自動分析、評估個人的行為習慣、興趣愛好或者經濟、健康、信用狀況等，並進行決策的活動（《保護法》第七十三條（二））。

個人信息處理者利用個人信息進行自動化決策時應當保證決策的**透明度**和結果的**公平**、**公正**，**並且不得對個人在交易價格等交易條件上實行不合理的差別待遇**（《保護法》第二十四條）。

通過自動化決策方式作出對個人權益有重大影響的決定，個人有權要求個人信息處理者予以**說明**，和**拒絕**個人信息處理者僅通過自動化決策的方式作出決定（《保護法》第二十四條）。

通過自動化決策方式進行信息推送、商業營銷時，應當同時提供不針對其個人特徵的選項，或向個人提供便捷的拒絕方式（《保護法》第二十四條）。

個人信息處理者應當在進行自動化決策前，進行個人信息保護影響評估，並將有關報告和記錄保存至少三年（《保護法》第五十五條至五十六條）。

17. 查閱及更正

個人有權向個人信息處理者查閱、複製其個人信息，個人信息處理者應當及時提供（《保護法》第四十五條）。

個人如發現其個人信息不準確或不完整，有權要求個人信息處理者更正、補充（《保護法》第四十六條）。

個人信息處理者應當建立便捷的個人行使權利的申請受理和處理機制。在拒絕個人行使權利的請求時應當說明理由。個人信息處理者如拒絕請求，個人亦可向人民法院提起訴訟（《保護法》第五十條）。

18. 個人信息可攜權

個人請求將個人信息轉移至其指定的個人信息處理者，如請求符合國家網信部門的規定條件，個人信息處理者應當提供轉移的途徑（《保護法》第四十五條）。

19. 刪除權、限制或拒絕個人信息處理

個人信息處理者應當主動或者根據個人的請求，在下列其中一種情況出現時**刪除**個人信息（《保護法》第四十七條）：

- 處理目的已實現、無法實現或者為實現處理目的不再必要；
- 個人信息處理者停止提供產品或者服務；
- 保存期限已屆滿；
- 個人撤回同意；
- 個人信息處理者違反法律、行政法規或者違反約定處理個人信息；
- 法律、行政法規規定的其他情形。

若刪除個人信息從技術上難以實現，個人信息處理者應當停止除了存儲和採取必要的安全保護措施以外的個人信息處理（《保護法》第四十七條）。

個人有權**限制**或**拒絕**他人對其個人信息進行處理，除非法律或行政法規另有規定（《保護法》第四十四條）。

已去世自然人的近親屬為了自身的合法、正當利益，可以對死者的相關個人信息行使查閱、複制、更正、刪除等權利（《保護法》第四十九條）。

20. 執法機構

國家網信部門負責統籌協調個人信息保護工作和相關監督管理工作，**國務院有關部門**在各自職責範圍內負責個人信息保護和監督管理工作（《保護法》第六十條）。

上述部門統稱為履行個人信息保護職責的部門（《保護法》第六十條）。

履行個人信息保護職責的部門在履行職責中，如發現違法處理個人信息涉嫌犯罪，應當及時移送公安機關依法處理（《保護法》第六十四條）。

21. 罰則

違反《個人信息保護法》規定處理個人信息，由履行個人信息保護職責的部門**責令改正**，給予**警告**，**沒收違法所得**。拒不改正的可處一百萬元以下**罰款**，對直接負責的主管人員和其他直接責任人員處一萬元以上十萬元以下罰款（《保護法》第六十六條）。

如屬**情節嚴重**，由省級以上履行個人信息保護職責的部門責令改正，沒收違法所得，並處**五千萬元**以下或者上一年度**營業額百分之五**以下罰款，並可以責令**暫停相關業務**、**停業整頓**、通報有關主管部門吊銷相關業務許可或者**吊銷**營業執照，對直接負責的主管人員和其他直接責任人員處十萬元以上一百萬元以下罰款，並可以禁止他們在一定期限內擔任相關企業的董事、監事、高級管理人員和個人信息保護負責人（《保護法》第六十六條）。

違反《保護法》規定，構成違反治安管理行為，依法給予治安管理處罰。構成犯罪可被依法追究刑事責任（《保護法》第七十一條）。

此外，有關違反《保護法》的行為亦可被記入信用檔案，並予以公示（《保護法》第六十七條）。

22. 民事索償

如處理個人信息侵害個人信息權益及造成損害，個人信息處理者不能證明自己沒有過錯的，應當承擔損害賠償等侵權責任。損害賠償責任按照個人因此受到的損失或者個人信息處理者因此獲得的利益確定。如個人因此受到的損失和個人信息處理者因此獲得的利益難以確定，則根據實際情況確定賠償數額（《保護法》第六十九條）。

個人信息處理者如違反《保護法》規定處理個人信息，並侵害眾多個人的權益，人民檢察院、法律規定的消費者組織、國家網信部門確定的組織可以依法向人民法院提起訴訟（《保護法》第七十條）。

有關《個人信息保護法》的全文，
可參閱全國人大網頁，或掃描二維碼：

http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml