Hutchison Telecommunications Hong Kong Holdings Limited
和記電訊香港控股有限公司

（於開曼群島註冊成立之有限公司）
（股份代號：215）

個人資料管理政策

I. 政策聲明

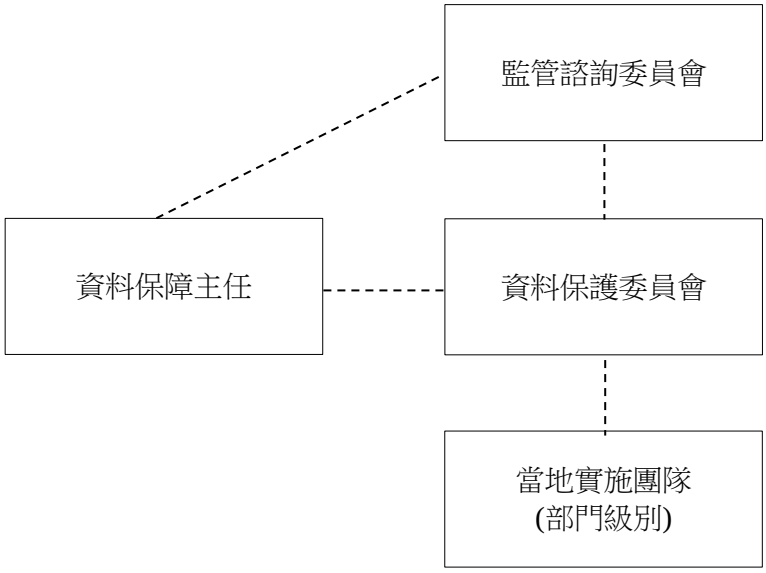
1.1 和記電訊香港控股有限公司 （「**和記電訊香港控股**」，聯同其附屬公司及受控制聯屬公司稱為「**集團**」），確認保護個人資料是維持客戶及僱員信任的關鍵。集團致力遵守適用資料保護法律及實施領先的資料保護標準，以保障及保護他們的個人資料。

1.2 本政策載列保障集團僱員及客戶個人資料的管理架構。本政策應與集團的資訊安全政策及操守守則以及其他政策及程序一併閱讀。

1.3 和記電訊香港控股的保護個人資料事宜由監管諮詢委員會負責，該委員會由資料保護委員會支援。集團的資料管理架構載於下文圖 1。

1.4 本政策適用於集團以及集團所有董事、行政人員及僱員。

圖 1 - 資料管理架構



1.5 有關本政策的任何問題，請聯絡法律及法規事務部或企業保安部。

1.6 附錄一載列本政策及構成資料管理架構其一部分的其他文件所用的常用詞彙及主要概念摘要。此外，個別的私隱政策亦會提供予供應商。

II. 管理架構

2.1 香港及澳門業務（各為一個業務單位，「業務單位」）的高級管理人員，須對有效實施本政策（包括下文所載的資料私隱原則及程序）負責。業務單位的高級管理人員須確保在（及遵守）適用資料保護法律的規限下，本政策獲併入及納入其他政策及程序。

2.2 作為其客戶及僱員個人資料的「資料管理者」，各業務單位必須以能夠證明遵守適用資料保護法律的方式實施當地政策及程序，包括（如需要）：

(a) 確保立法及監管規定獲納入涉及處理個人資料的所有活動中（如確保涉及處理個人資料的所有新項目有「保護私隱的設計」）；

(b) 實施適當的技術及機構措施，旨在有效實施資料私隱原則及在處理活動中加入必要保障，並按照其營運所在司法管轄權區的規定保護資料當事人的權利；

(c) 定期為僱員提供保護私隱及資料意識的培訓，以確保他們關注及了解本政策，以及他們在保護資料管理及私隱方面的責任；

(d) 定期評估業務做法和技術的私隱風險，以衡量私隱風險（包括與第三方供應商有關的風險）及緩和控制措施是否充足；

(e) 確保個人資料按其敏感度分類及處理，並按知情需要限制存取；及

(f) 指派適當的私隱及資訊科技安全專家，支援業務管理資料私隱風險（如委任資料保護人員）。

2.3 所有涉及處理個人資料的僱員均應了解及遵守本政策，以及其業務單位實施的任何相關政策、程序及指引。未有按照本政策處理個人資料或會導致紀律行動，嚴重及／或故意違反本政策者或會被解僱。

III. 資料私隱原則

集團任何時候均應按照以下資料私隱原則處理個人資料。

3.1 合法、公平及透明地處理

(a) 僅會以合法、公平及透明的方式使用個人資料。

(b) 個人資料的使用應遵守集團營運所在各司法管轄權區內的適用資料保護法律。集團對於處理客戶及僱員個人資料的時間、方式及目的，以及個人在該司法管轄權區就其個人資料的處理擁有哪些選擇及權利須保持透明。

(c) 個人資料的存取應僅限於僱員需要知悉有關資料以履行其在集團之職務，而敏感個人資料（包括其存取）需獲得最高程度保護。

3.2 目的及用途

個人資料僅應基於特定、明確及合法的目的並在需要達到該等目的時收集。使用個人資料有助改善集團提供的服務，但使用該等資料應具有明確目的。

3.3 資料準確性

應採取合理措施確保持有的任何個人資料屬準確及最新。

3.4 保留資料

個人資料應僅於有必要保留以履行其指定用途的期間保存。各業務單位應向相關管理人員及員工發出有關文件保留期的指引。

3.5 刪除資料

除非任何適用法律禁止刪除，或不刪除資料乃符合公眾利益，否則於所持有資料毋須再用作其收集目的時（包括任何直接相關目的）， 集團應採取一切切實可行的措施刪除有關個人資料。

3.6 個人的權利

(a) 個人資料應按照業務單位營運所在各司法管轄權區內適用資料保護法律下的個人權利處理。

(b) 個人對存取、修改、刪除或其他涉及其個人資料的所有要求，應符合適用資料保護法律的方式處理，並按適當程序接收及回應該等要求。

3.7 資訊安全

(a) 應採取適當的技術及機構保安措施，保障受託於集團的個人資料免受未經許可或非法處理，並避免意外遺失、損毀或損壞，以確保與風險切合的安全水平（如個人資料採用假名及加密及／或其他適當的安全措施）。

(b) 應定期檢討安全措施，以確保其提供適當的保護水平。

(c) 應採用同等的安全水平保護代表第三方處理的個人資料（如業務單位擔任「資料處理者」）。

3.8 跨境傳送個人資料

集團可能有需要將資料轉移至非業務單位營運所在的司法管轄權區。個人資料不應傳送至未有提供充足資料保護或並無適當保障的國家或地區。

IV. 程序

各業務單位須實施適當的程序，確保個人資料按照資料私隱原則及適用資料保護法律公平及合法地處理。

4.1 處理記錄

如適用資料保護法律有所規定，各業務單位應保存處理活動的記錄及有關遵守資料保護的文檔。

4.2 私隱影響評估

如適用資料保護法律有所規定或在管理私隱風險的適當情況下，應對新產品、技術及業務營運進行私隱影響評估。例如，如項目涉及以下一項或多項：處理大量個人資料或該等處理影響大量個人；將現有個人資料用作全新及／或更具侵犯性的目的；處理敏感個人資料及／或遺傳或生物特徵資料（如指紋掃描、人臉識別）；引入全新及侵犯性的技術（如閉路電視錄影機、定位技術）；或從事任何類型的僱員監察（包括任何記錄及／或審查僱員的通訊或活動，包括電話通話、電子郵件及電腦文件）。

4.3 私隱通知

如適用資料保護法律有所規定，各業務單位應實施適當的私隱政策／通知（「**私隱通知**」），包括向客戶及僱員解釋處理的個人資料類別及目的。該等私隱通知應隨時可供查閱及保持更新，如法律有所規定，應備有簡單機制供個人選擇不處理或不同意處理其個人資料。

4.4 資料當事人要求

個人對存取、修改、刪除或其他涉及其個人資料的所有要求，應按照符合適用資料保護法律的程序處理。

4.5 向執法機構／其他監管機構披露個人資料

集團可能有責任在若干特定及有限情況下向執法機關或其他監管機構披露個人資料。回應有關個人資料的正式要求應與保護個人資料的義務作出平衡。所有僱員必須遵守相關程序，如有疑問，必須諮詢法律及法規事務部及企業保安部。

4.6 與私隱執法機構合作

集團致力配合私隱執法機構的查詢及調查，特別是如其關注集團僱員、客戶或網站用戶的私隱。私隱執法機構發出的通訊應立即轉介至法律及法規事務部及企業保安部處理。

4.7 資料安全事故

當發生涉及個人資料的資料安全事故（「**資料安全事故**」）時，業務單位應致力盡快減輕潛在後果並確保個人資料免受進一步未經許可存取、使用或損壞。業務單位應迅速及按照適用資料安全事故程序作出回應，當中可能包括通知私隱執法機構及／或受影響個別人士（如需要）。如資料安全事故涉及個人資料，應立即通知法律及法規事務部及企業保安部。應不時發出通知及處理資料安全事故的進一步指引。

4.8 使用閉路電視

使用閉路電視可能涉及處理個人的可識別影像。使用時，業務單位必須考慮安裝閉路電視及處理所收集資料時所攝錄影像的潛在敏感性質。涉及使用閉路電視的僱員應接受有關使用的培訓，確保符合適用資料保護法律。

4.9 第三方處理者

如在涉及處理個人資料的部分業務營運中委聘第三方服務供應商，則必須確保：

(a) 在篩選有關供應商時已進行適當審查，並持續監察及檢討該等第三方供應商；

(b) 該第三方按照本政策採取充足的私隱及安全保障措施；

(c) 於開始處理前已擬定包括資料私隱條款的合約，並經法律及法規事務部批准；及

(d) 採納有關聘用第三方處理者之私隱影響評估得出的任何建議（如適用）。

4.10 資料當事人提出關注的機制

業務單位應維持清晰及可查閱的機制，以便資料當事人就資料隱私提出關注。

(2024 年 5 月)

首次採納：2014年9月
首次更新：2020年7月
第二次更新：2021年11月
第三次更新：2024 年 5 月

附錄一　　詞彙及主要概念

詞彙

詞語	釋義
適用資料保護法律	指相關國家確保保護個人資料的適用法律及規例。
生物特徵資料	指包含或連結到個人的行為和生理特徵的個人資料，可用於識別、標記或描述該人，包括但不限於脫氧核糖核酸、指紋、面部形狀、視網膜和虹膜模式、手部掃描和測量以及語音檔。
機密	指若無意中或未經許可披露，可能會對個人的私隱產生重大負面影響的資訊。
客戶	指集團貨品及服務的所有客戶、顧客及買家，包括相關客戶會員計劃的會員（不論線上及／或線下）。
資料管理者	指獨自或與他人共同決定處理個人資料目的及方法的實體。
資料私隱人員	指負責管理集團內遵守適用資料保護法律的員工或服務提供者。
資料處理	指對個人資料作出的任何操作（不論是否利用自動方式），包括收集、記錄、組織、儲存、修改或更改、檢索、諮詢、使用、披露、提供、排列、合併、限制、刪除及銷毀個人資料。
資料處理者	指代表資料管理者處理個人資料的自然人或法人、公共機構、代理機構或任何其他實體（而資料處理的定義應按本釋義詮釋）。
資料保護原則	指相關適用資料保護法律中所定義的原則。
資料安全事故	指集團資料的安全、機密、完整或提供已經或可能受損的任何實際或懷疑事件。例如：資料或儲存集團資料的設備遺失或被竊、共用或不當使用密碼，以致未經許可存取集團資料、資訊科技系統故障、人為錯誤、不可預見的情況（如火災或水災）、集團的資訊科技系統遭黑客攻擊、不當處理或處置集團資料及透過欺詐獲得集團資料的罪行。
資料當事人	指集團業務單位持有其個人資料的個人。

詞語	釋義
僱員	指為集團或其任何業務實體工作的所有人士，包括持有臨時、定期及永久僱傭合約的僱員。
遺傳資料	指與個人遺傳特徵有關的所有個人資料。
集團資料	指有關集團潛在、現有及／或前客戶、供應商、僱員及網站用戶的資料，及／或集團任何其他機密資料（包括個人資料）。
個人資料	指直接或間接可識別一名個別人士（不論是客戶、僱員或集團或業務單位網站的用戶）的資料。
私隱執法機構	指相關國家負責管理及執行相關適用資料保護法律的資訊專員公署或同等監管機構。
敏感個人資料	指基於其敏感性質而在處理時受到額外法律管制的任何個人資料，包括以下特殊類別的個人資料：關於個人種族或民族起源、思想意識或政治觀點、宗教或哲學信仰、工會會員、身體或精神健康、性生活或取向、刑事定罪或涉嫌干犯任何罪行的資料，以及任何遺傳資料或生物特徵資料。

主要概念

主要釋義及概念

何謂「處理」?

適用資料保護法律監管「處理」個人資料。處理的定義非常廣泛，並涵蓋接收、持有、儲存、收集、刪除、修改、編輯、銷售、分析或匯報個人資料等一系列活動。該等規則適用於持有電腦數據庫、經文檔處理的文件及錄音帶內的資料，或錄影帶、CD、DVD 或以數碼影像形式儲存可識別人物的影像。適用資料保護法律亦監管以檔案系統持有的紙張資訊。

何謂「個人資料」?

如資料有關(a)從該等資料中，或(b)從我們管有或很可能管有的該等資料及其他資訊中可以「識別」或「可予識別」在世的個人，該資料即為個人資料。因此，個人資料的概念極其廣泛。在某些國家，與公司實體有關的資料乃被視為個人資料。

例子：如一個電話號碼可以識別在世的個人，則該電話號碼本身可能是個人資料。信用卡載有的資訊構成個人資料，因為其載有持卡人的姓名。錄影機內的片段如可識別個人，便可視為個人資料。電話或電子郵件記錄資料包含個人資料，因為可以直接或間接識別進行通訊的個人。

個人資料亦包括對個人的意見的任何表達以及集團或任何其他人士就該個人的意向的任何指示。

何謂敏感個人資料?

敏感個人資料指處理時受到額外法律管制的各類型資料，並包括關於個人種族或民族起源、思想意識或政治觀點、宗教信仰或類似性質的其他信仰、工會會員、身體或精神健康狀況、性生活、干犯或涉嫌干犯任何罪行、干犯或涉嫌干犯任何罪行的任何訴訟以及相關訴訟結果的資料。請注意，在某些司法管轄權區，有關定義可能更為寬泛，而在某些司法管轄權區，與犯罪及訴訟有關的資訊將構成「司法資料」並須遵守特定規則。許多國家對處理敏感個人資料及司法資料有更嚴謹的規則。如集團依賴同意處理敏感個人資料，該同意必須「明確」，即個人需要採取一些主動步驟以顯示其接受。

何謂好的資料管理?

適用資料保護法律亦規定須制定良好的資料管理程序，以確保個人資料獲妥善處理（(如個人資料屬準確和最新 ）。任何不再需要、已過期或不準確的資料應予刪除。

資料管理者與資料處理者有何分別?

資料管理者是管理收集資料的方式及目的的實體，即使其本身並非實際持有資料。因此，即使資料由代表業務單位行事的第三方持有（如工資管理外判予第三方），業務單位將是有關其僱員或客戶資料的資料管理者。代表資料管理者持有及處理個人資料的人士是**資料處理者**。如業務單位聯同另一人士管理處理的方式及目的，雙方可為聯合資料管理者。

例子：業務單位有若干市場推廣資料希望處理及發佈以發展品牌。第三方代理機構代表業務單位並按其指示進行處理（如發送直接市場推廣通訊）。業務單位為資料管理者，而代理機構將為資料處理者。