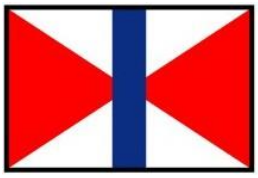

太古公司

集團個人資料政策及指引

二零一九年九月

Internal use only

A. 政策

1. 目的

1.1 本文件載有太古公司有關個人資料的政策及一般指引。

1.2 在本文件中：-

(a) 「**個人資料**」是指任何與一個被確定或可被確定身分的人士（如顧客、員工等）有關的資料（如姓名、聯絡資料、護照號碼、生物特徵、健康資料等）；

(b) 凡提述「**太古公司**」，均指太古股份有限公司及其附屬公司（各為一「**太古系公司**」；

(c) 凡提述「**相關人員**」，均指太古公司的所有員工；及

(d) 凡提述「**部門**」，均指按下述部門劃分而成的太古系公司組合：(i) 地產，(ii)航空（為免存疑，不包括國泰航空），(iii)飲料，(iv)海洋服務，及(v)貿易及實業。

1.3 其他釋義請參閱本文件 **J 部分**。

2. 公司政策

2.1 太古公司的政策是遵守有關處理個人資料（包括收集、持有、處理、披露及使用個人資料）的適用法律規定（「**適用個人資料法規**」）。在業務過程中，必須尊重他人的私隱及對收集所得的資料保密。

2.2 不遵守適用個人資料法規可能會構成罪行，並可能導致太古公司及/或相關人員被處以罰款及 / 或監禁。太古公司亦可能因不遵守適用個人資料法規而遭受商業、聲譽或其他方面的不利影響。

2.3 本文件 **B 至 I 部分**列明有關處理個人資料的一般指引，部門應遵守該等一般指引。

2.4 部門應仔細審視其現行運作，並遵守適用個人資料法規的任何其他相關規定。

Internal use only

B. 保障資料主任

1. 保障資料主任的委任

1.1 部門應委任一名保障資料主任（「**保障資料主任**」）。保障資料主任的任命應基於其專業質素及對個人資料法例及慣例的專業知識而作出，其職責為監察有關部門在遵守適用個人資料法規的情況。

2. 保障資料主任的職責

2.1 具體而言，保障資料主任應負責：

(a) 制定詳細的個人資料管治政策、指引、標準，及適用於其部門的程序（「**部門指引**」），以確保遵守適用個人資料法規；

(b) 協調其部門內各業務單位執行部門指引；

(c) 審核及批准私隱影響評估（按 C1.1 部分的定義）；

(d) 為其部門制定事故應變計劃及程序。該等計劃及程序應涵蓋資料外洩事故，並應就資料外洩事故的妥善處理、升級及滙報為部門高級管理人員提供指引。

(e) 不時舉辦有關個人資料的培訓，以提高員工的意識；及

(f) 適用個人資料法規可能要求保障資料主任履行的其他職務。

Internal use only

C. 收集個人資料

1. 私隱影響評估

1.1 在收集個人資料**之前**，部門**應進行一次私隱影響評估**（「**私隱影響評估**」），對建議進行的收集行動加以評估，以避免或減低對私隱構成的不利影響。有關私隱影響評估一般應包括的詳細內容，請參閱**附件Ⅰ**。

1.2 在收集個人資料之前，私隱影響評估應先經保障資料主任審核及批准。

2. 收集個人資料

一般原則

2.1 部門僅應為與其職能或活動**直接有關的合法目的**而收集**必需的**個人資料，收集個人資料**不得超乎適度**。

2.2 個人資料只應以**合法和公平**的方式收集。

2.3 根據適用個人資料法規，個人資料可分為不同類別（如敏感個人資料及兒童個人資料等）。部門應遵守適用個人資料法規對處理不同類別個人資料的其他法律規定。

個人資料收集聲明

2.4 在收集資料當事人的任何個人資料**之時或之前**，太古系公司**應**向資料當事人**提供或出示個人資料收集聲明（「個人資料收集聲明」）**。個人資料收集聲明應**以清晰而顯眼的方式**提供或展示。

2.5 個人資料收集聲明的目的，是為資料當事人提供有關收集及處理其個人資料的相關資訊，包括：-

(a) 收集個人資料的**目的**（即個人資料的用途）；

(b) 部門可能將個人資料轉移予**哪類人士**（非作直接促銷用途）；

(c) 資料當事人是**有責任還是可自願**提供其個人資料。如為有責任提供資料，應列明不提供資料的後果；

(d) 倘部門擬使用收集所得的個人資料作直接促銷用途，則須：-

(i) 將該意圖告知資料當事人；
(ii) 告知資料當事人，部門不可在未經資料當事人同意下使用其資料；
(iii)就擬使用甚麼種類的個人資料（如姓名及電郵地址）（「**個人資料種類**」）作直接促銷用途提供相關的**特定**資訊；
(iv)就擬將個人資料用於甚麼類別的促銷標的（如 ABC 公司提供的美容產品）（「**促銷標的類別**」）提供相關的**特定**資訊；
(v) 說明資料當事人可（免費）傳達其同意的回應途徑（如電郵或郵寄地址）。

(e) 有關的太古系公司如擬將收集所得的個人資料轉移或提供予第三者（包括另一太古系公司）作直接促銷用途，則須：-

(i) 將該意圖告知資料當事人；
(ii) 告知資料當事人，收集資料的太古系公司不可在未經資料當事人書面同意下轉移或提供該等資料；
(iii)（如適用）告知資料當事人，其個人資料將是**為得益**（即為換取金錢或其他財物）而轉移或提供的；
(iv)提供以下**特定**資訊：(A)擬轉移或提供的個人資料種類，(B) 擬轉移或提供個人資料予甚麼類別的人士（如促銷或調研服務供應商）（「**人士類別**」），及(C) 擬使用資料的相關促銷標的類別；

(f) 資料當事人根據適用個人資料法規享有的**權利**（如查閱及改正資料的權利）；

(g) 負責處理資料查詢或要求的人士（如保障資料主任）的**姓名（或職銜）及聯絡資料**；及

(h) 根據適用個人資料法規須向資料當事人提供的其他資料。例如，對於人士類別，若干適用個人資料法規要求在個人資料收集聲明中列明獲轉移資料的公司全名（如 ABC 有限公司）。

2.6 各部門應考慮是否須按適用個人資料法規的規定取得資料當事人對個人資料收集聲明及 / 或擬使用或轉移其個人資料而作出的一般、特定及 / 或書面同意。

Internal use only

向第三者收集資料當事人的個人資料

2.7 如要向第三者（而非直接向資料當事人）收集資料當事人的個人資料，部門應考慮是否須按適用個人資料法規的規定向第三者取得（有關第三者遵守適用個人資料法規對轉移及使用個人資料的規定等的）書面確認。

3. 資料私隱政策

3.1 部門應制定載有下述資訊的公開政策或聲明（「**資料私隱政策**」）：

(a) 部門有關個人資料的政策及做法；

(b) 部門持有的個人資料種類；

(c) 部門持有個人資料的主要目的；及

(d) 按適用個人資料法規的規定須予公開的任何其他資訊。

3.2 為確保任何人士可清楚知道部門有關個人資料的資料私隱政策，有關部門應在其所有網站上以清晰而顯眼的方式顯示其資料私隱政策。

3.3 如認為合法及適宜，部門可將個人資料收集聲明及其資料私隱政策合併為一份文件。

4. 小型文字檔案（Cookie）及其他追蹤網上行為的技術

4.1 追蹤網上行為包括透過使用 cookie 或其他技術記錄使用者的身份、買賣及/或網上行為。

4.2 如部門進行網上行為追蹤，應遵守適用個人資料法規的相關規定，或會包括在進行網上行為追蹤活動的網站上刊登 cookie 政策。

Internal use only

D. 個人資料的使用及轉移

1. 使用個人資料

1.1 部門應**只可為告知資料當事人的目的**而使用、披露、處理或轉移個人資料（及如適用的話，資料當事人已對該使用目的給予同意）。

1.2 如為其他目的（即「新增目的」）而使用、披露或轉移個人資料，相關的太古系公司**必須事先取得**資料當事人的**同意**。

1.3 不同的適用個人資料法規對使用及轉移若干類別的個人資料（如敏感個人資料及兒童個人資料）可能訂有較為嚴謹的規定，部門應仔細審視適用個人資料法規的規定並予以遵守。

2. 使用可公開獲得的個人資料

2.1 如第三者（如專業團體）公開某些個人資料（如電話簿）並指明可使用該等資料的目的（如進行業務聯繫），相關的太古系公司僅可為指定目的而使用該等個人資料。如未有註明目的，相關的太古系公司應考慮個別人士對私隱的合理期望（即一個合理的人是否會認為相關資料被再用是超乎預期或不恰當的）。

2.2 部門從公共領域收集的個人資料不得用於直接促銷用途。

3. 向第三者轉移個人資料

3.1 向第三者（包括太古系公司）轉移任何個人資料之前，作出轉移的太古系公司應告知該第三者，向其提供個人資料的目的。有關目的應為作出轉移的太古系公司向相關資料當事人提供的個人資料收集聲明所列明的任何目的，以避免第三者濫用資料。

3.2 根據若干適用個人資料法規，在轉移任何個人資料之前，可能需要與第三者簽訂書面協議，對第三者施加保障資料的責任。

3.3 請各部門遵守本文件中有關將個人資料轉移給第三者的其他適用規定（如本文件 **E 部分**的資料處理規定）。

4. 從第三者取得個人資料

4.1 從第三者（包括太古系公司）取得任何個人資料之前，取用資料的太古系公司應要求第三者指明個人資料可能用於哪些目的。部門請審視是否須按適用個人資料法規的規定與第三者簽訂有關該資料轉移的書面協議。

4.2 如相關的太古系公司擬使用從第三者取得的個人資料作直接促銷用途，應先就下述事宜**向第三者取得書面確認**：

(a) 第三者已遵守有關轉移或披露個人資料的適用個人資料法規；

(b) 第三者已就轉移或披露個人資料向資料當事人**發出書面通知**及**取得其書面同意**；

(c) 部門對個人資料的使用與第三者從資料當事人取得的同意相符；及

(d) 根據適用個人資料法規，部門須在使用個人資料作直接促銷用途前從第三者取得的任何其他確認。

5. 跨境轉移個人資料

5.1 不同的司法管轄區對個人資料的跨境轉移有不同的法規。例如，根據某些適用個人資料法規的規定，個人資料被轉移到外地前須取得認證及符合已核准的行為守則。部門應審閱適用個人資料法規以確保合規。

E. 資料處理

1. 簽訂合約前的盡職審查

1.1 部門在聘請資料處理主任之前，應對有關資料處理主任進行盡職審查。

1.2 部門應考慮有關資料處理主任是否適合獲委聘出任有關職位。資料處理主任應具備相關能力和經驗，並採取足夠的技術和保安措施以保障個人資料。

2. 合約安排

2.1 將任何個人資料轉移予資料處理主任之前，相關的太古系公司必須確保與資料處理主任簽訂書面協議。

2.2 書面協議應對資料處理主任施加下述保障資料的責任：-

(a) 如不再需要使用個人資料作資料處理用途，應適時將有關資料退還、銷毀或刪除 。如適當和可行，指名合理的期限內資料處理主任須把個人資料退還、銷毀或刪除；

(b) 採取適當及必要的保安措施以保障個人資料，防止有關資料被人未獲准許地或意外地查閱、處理、刪除、遺失或使用；

(c) 禁止使用（或披露）個人資料作執行資料處理職責以外的任何用途；

(d) 絕對禁止（或在有限制下容許）將資料處理服務分判。如容許分判，資料處理主任的協議應對分判商施加相同的責任。如分判商未能履行其責任，資料處理主任須負全責；

(e) 如發現有任何不尋常或保安違規情況，即時向部門報告；

(f) 採取措施確保其相關員工執行保安措施，並遵守上述責任（如資料處理主任應制定個人資料保障政策，並為其相關員工提供足夠培訓）；

(g) 容許部門就資料處理主任如何處理和儲存個人資料進行審核和視察；

Internal use only

(h) 遵守適用個人資料法規的所有相關規定；及

(i) 違反合約須承擔責任，並訂明違反合約的後果。

Internal use only

F. 資料的準確性、保留期及刪除

1. 資料的準確性

1.1 部門應採取所有切實可行的步驟，以確保在考慮到**有關的個人資料會用於甚麼目的**（「**目的**」）後，所持有的資料是**準確**的。

2. 資料的保留期

2.1 部門應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**將其保存以貫徹其使用目的**所需的時間**。

2.2 部門應制定保留期的政策，訂明其所持有的個人資料的保留期。

3. 資料的刪除

3.1 在下述情況下，部門應採取所有切實可行的步驟，將所持有的個人資料刪除 (a) 該等資料**不再需要**用於目的；或 (b) 在部門認為適當的範圍內或在法律規定的情況下，由資料當事人提出刪除要求。

3.2 個人資料必須在**妥善和保安良好的情況下**銷毀或刪除。在棄置載有個人資料的儲存裝置時，應採取切實可行的步驟以確保資料已刪除且不可再取閱。

3.3 部門應制定妥善刪除個人資料的程序(包括確定和收集副本的方式)，並保存刪除紀錄。

Internal use only

G. 個人資料的保安

1. 一般原則

1.1 部門應採取所有切實可行的步驟，以確保在考慮下述各項後，個人資料受到保障，不會被人**未獲准許地查閱、更改、遺失或處理**：-

(a) 該資料的種類及可能做成的損害；

(b) 儲存該資料的地點；

(c) 儲存該資料的設備所採取的保安措施；

(d) 為確保能查閱資料的員工是適合人選所採取的措施；

(e) 為確保在保安良好的情況下傳送資料所採取的措施。

2. 存取控制

2.1 個人資料必須在基於**「有需要知道」及「有需要使用」原則**下進行查閱。部門應 (a) 決定其員工的查閱權限；及 (b) 實施妥善的查閱授權及核實程序。

2.2 部門負責提醒其員工有關個人資料私隱及保安事宜，且必須信納已向能查閱個人資料的員工充分簡述該等事宜。

3. 儲存 / 保安措施

3.1 個人資料（不論任何形式）必須時刻**在保安良好的情況下儲存**。不應建立或保存不必要的個人資料副本。

3.2 部門應採取適當的保安措施，以保障個人資料不會受到未獲批准的查閱或更改。

Internal use only

H. 資料當事人的要求

1. 查閱資料要求

1.1 資料當事人有權確定一家太古系公司是否持有其個人資料，若然，則有權獲取一份有關資料的副本。

1.2 部門應根據適用個人資料法規，按照訂明的限期在有關期間遵從資料當事人的查閱資料要求。

2. 改正資料要求

2.2 資料當事人可要求更正其個人資料。

2.3 如舊的個人資料不準確，(a) 應按照資料當事人的要求作出所需的改正；及 (b) 應在適用個人資料法規所訂明的限期內，向資料當事人提供一份經改正的個人資料複本。

3. 拒絕直接促銷服務要求

3.1 如資料當事人要求一家太古系公司停止在直接促銷中使用其個人資料（或停止提供其個人資料予他人使用）（「**拒絕直接促銷服務**」），部門應相應地遵從該項要求。

3.2 部門應備存有關所有拒絕直接促銷服務資料當事人的名單，並定期更新該等名單。

4. 其他要求

4.1 根據適用個人資料法規，資料當事人可享有其他權利（如資料刪除／遮蓋要求、被遺忘權、限制處理權及 / 或資料可攜權）。部門應審視其運作，並遵守適用個人資料法規的相關要求。

I. 資料外洩的處理

1. 資料外洩的定義

1.1 資料外洩是指部門（或其資料處理主任或資料共同擁有者）所持有的個人資料保安不足，以致洩露資料。

1.2 資料外洩的例子如下：-

- 遺失載有個人資料的儲存裝置
- 意外地或未獲批准地傳送或披露個人資料
- 載有個人資料的數據庫被黑客入侵

2. 事故應變計劃

2.1 部門應制定事故應變計劃，就處理資料外洩事故列明下述各項：-

(a) 成立及籌組一個事故應變組；

(b) 事故應變組成員各自的角色和責任；

(c) 上報程序、通訊及應變行動（包括損害控制）；及

(d) 調查及事故後分析。

2.2 部門在考慮到適用個人資料法規後，應考慮是否需要或適合向資料當事人及/或相關監管機構發出資料外洩通知。

Internal use only

J. 定義

下述詞彙儘管屬常用詞彙，但其定義可能因不同法域而有所差異。以下列出的定義詞彙可供參考，部門應根據適用個人資料法規審視其相應的定義。

「**資料處理主任**」	指符合以下兩項說明的人：- - 代另一人處理個人資料；及 - 並不為該人本身目的而處理該資料。 *例如，受委聘代另一人將個人資料輸入電腦系統或將載有個人資料的機密文件碎掉的服務公司。*
「**資料當事人**」	指屬該個人資料的當事人的個別人士（如顧客、僱員等）。
「**直接促銷**」	指：- - 向一個人士要約提供貨品、設施或服務，或為該等貨品、設施或服務可予提供而向一個人士進行廣告宣傳，或 - 為慈善、文化、公益、康體、政治或其他目的向一個人士索求捐贈或貢獻。
「**促銷標的**」	就直接促銷而言，指：- - 被要約提供或就其可予提供而進行廣告宣傳的任何貨品、設施或服務，或 - 任何索求捐贈或貢獻的目的。
「**處理**」	指對個人資料進行的任何操作（不論是否藉自動化方法進行）。 *例如，將個人資料收集、記錄、分析、彙編、修訂、擴增、刪除、組織、儲存、取閱、重新排列、使用、披露、發佈、組合、限制、刪除或處置。*

附件 I
私隱影響評估

私隱影響評估至少應包括下述各項：-

1. 資料處理周期分析

1.1 審視項目背後的**目的**和**理據**，以決定**是否需要**收集該等**種類**、**數量**和**範圍**的個人資料。

1.2 在切實可行的範圍內，採納私隱侵犯程度較低的替代方式和方法。

1.3 確保本文件列載的指引及部門指引獲得遵從。

2. 私隱風險分析

2.1 分析相關私隱風險。進行分析時，應考慮下述各項：-

(a) 部門內太古系公司的職能和活動；

(b) 性質及所涉的個人資料；

(c) 受影響的人數；

(d) 資料當事人的個人資料如處理不當，對其所造成傷害的嚴重程度；

(e) 資料處理主任是否獲（或將獲）委託進行資料處理；及

(f) 適用個人資料法規及部門須依循的任何適用實務守則、指引及規例等所訂明的私隱標準和規則。

2.2 一般而言，部門須採取的個人資料保障措施的程度，應與項目的私隱侵犯性相稱。

3. 避免或減輕私隱風險

3.1 在切實可行的範圍內，**避免**私隱風險或**採納適當的減輕私隱風險措施**，以保障個人資料，防止有關資料被人未獲准許地查閱、處理、刪除、遺失或使用。

4. 清晰的書面紀錄

4.1 私隱影響評估應有清晰的書面紀錄。書面紀錄應包括評估結果、建議，以及就項目擬採納的減輕私隱風險措施。

4.2 私隱影響評估報告可包括下述各項：-

(a) 項目的敍述；

(b) 資料處理周期分析闡述（由資料使用者或其代理人）收集及處理個人資料的情況；

(c) 確定相關的私隱風險；及

(d) 妥善應對或減輕該等風險的方式和方法，並（以詳盡細節）解釋已經如何考慮其他私隱侵犯程度較低的替代方式和方法，以及（如適當）未有採納該等替代方式和方法的原因。

Internal use only