保險業辦理電子保單簽發作業自律規範

金融監督管理委員會 103.08.26 金管保綜字第 10302093141 號函及金管保綜字第 10302093142 號函准予備查

第一章 總則

第一條

為落實保險業簽發電子保單之紀錄保存、內部安全控制及契約範本等作業之管理，依據保險業設立許可及管理辦法第二十二條第二項規定訂定本自律規範。

第二條

保險業簽發電子保單除法令另有規定外，應依據本自律規範辦理。

前項所稱電子保單係指保險業與要保人訂立保險契約，並約定以電子文件方式簽發之保險單或暫保單。

第二章 紀錄保存

第三條

保險業簽發電子保單者，應至少保存下列項目之紀錄：

一、保險業向憑證機構申請使用、變更或廢止憑證等相關紀錄。

二、憑證載具啟用紀錄。

三、與簽發電子保單有關之所有交易資料紀錄。

第四條

保險業保存現有和已歸檔之電子保單相關交易資料紀錄時，應使用加密之特定媒體儲存或委託公信第三者保存，並定期製作備份資料。

第五條

已歸檔儲存之電子保單相關交易資料紀錄（以下簡稱歸檔資料），其保存期限於保險契約期滿或終止後至少五年；用以處理歸檔資料之應用程式保存期限亦同。

已逾保存期間之歸檔資料如欲銷燬，應採取適當之安全防範措施，避免洩漏個人資料。

第六條

保險業管理電子保單之歸檔資料，應依下列原則控管：

一、不得新增、修改或刪除歸檔資料。

二、必要時得將歸檔資料移至另一儲存媒體儲存，但應提供適當的保護，且保護等級應不低於原保護等級。

三、歸檔資料應存放於安全處所。

四、歸檔資料之管理應訂定相關作業程序。

五、應對歸檔資料之歸檔時間加以紀錄及管理。

六、欲取得歸檔資料者，除法令另有規定外，須提出申請並經允許後始得為之。歸檔資料之調閱，如涉及個人資料者，應依個人資料保護法相關規定辦理，未涉及個人資料者，則依內部調閱程序辦理。

第三章 內部安全控制

第七條

保險業對於電腦網路設備安全之防護，應符合下列條件：

一、所有電腦網路設備應安置於安全地點。

二、安置電腦網路設備之地點應加裝不斷電系統或備用發電機，並依法令規定設置必要及合格之消防安全設施。

三、安置電腦網路設備之地點應建立安全維護及人員進出之控管機制。

第八條

保險業簽發電子保單者，應就網路管理之緊急事故應變與災害復原處理訂定下列程序：

一、緊急事故通報程序。

二、緊急事故應變程序。

三、災害復原程序。

四、測試程序。

第九條

為確保電子保單資訊安全，保險業應訂定網路安全規劃與管理作業，以達成整體網路作業之安全管理。

前項網路安全規劃與管理作業應包括下列項目：

一、網路安全政策。

二、網路安全服務管理。

三、網路安全連結。

四、主機設備安全防護。

五、身分識別和驗證。

六、網域劃分與安全控制。

七、防火牆安全管理。

八、遠端連線控制。

九、網路安全監控。

十、監控處理程序。

十一、事件安全記錄。

十二、入侵偵測檢視。

十三、防範電腦病毒及惡意軟體之攻擊。

第十條

保險業應依下列原則管理負責電子保單作業之人員：

一、就資訊系統與人員之管理及權責分工訂定相關作業辦法， 並與員工簽署書面約定及定期宣導，以提醒員工注意。

二、訂定人員違反資訊安全規定之處理程序，並明訂處理電子保單相關交易資料之授權處理層級。

三、作業人員應定期接受有關資訊安全之訓練，並作成紀錄。

第十一條

保險業處理電子保單業務，如有依據保險業作業委託他人處理應注意事項辦理時，除依據第七條規定辦理外，應遵循下列原則：

一、事先研擬委外服務計畫書。

二、慎選具有足夠安全管理能力及經驗之廠商作為委辦對象。

三、事前審慎評估可能潛在之各項風險。

四、與委外廠商簽訂適當的資訊安全協定及課予相關安全管理責任，並納入契約條款。

五、逐年檢討評估委外廠商之履約情形，如有未履行或未達約定之服務水準者，應要求檢討改進，必要時得終止部分或全部契約，並依法追究其責任。

第十二條

保險業之電子保單安全稽核，應至少包含下列項目：

一、是否留有足供安全稽核之記錄資訊。

二、是否已建立防範不法入侵之機制。

三、是否已建立安全修復機制。

四、是否有定期更新修補程式。

五、是否已建立警示系統，對於安全違例事件的發生能立即採取有效防範措施。

第四章 數位簽章作業管理

第十三條

保險業以電子文件方式簽發保險單或暫保單時，應以數位簽章簽署。

保險業應與要保人約定以電子文件方式簽發保險單或暫保單，並列入「保險業內部控制制度及內部稽核作業手冊」中，以作為日後稽核之依據。

第十四條

保險業採用數位簽章時，應與憑證機構簽訂契約，並依本規範之規定辦理。

第十五條

保險業採用數位簽章機制時，應擬訂緊急應變計畫，以避免影響要保人之權益。

第十六條

保險業應依下列標準選擇憑證機構：

一、憑證機構之組織及性質

(一)依公司法設立、辦理公司登記且符合相關營業項目之股份有限公司。

(二)以網路認證服務為主要營業項目。

(三)須具備公信第三者之特性。

(四)所發行之憑證已符合電子簽章法及相關法令之規定。

二、憑證機構之數位簽章機制

(一)作業制度已符合電子簽章法及相關法令之規定。

(二)簽章金鑰（公開金鑰及私密金鑰）長度不低於 1024 位元（bits），加密金鑰長度不低於 40 位元（bits）。

三、憑證機構簽證電腦系統之安全性

(一)憑證機構簽發憑證之私密金鑰（Private Key）須儲存於硬體亂碼化設備，任何情況下均不得以明碼方式輸出於硬體設備之外。

(二)擁有自有之獨立機房及憑證簽發營運系統，具備嚴謹之安全設施，並不得與其他業務共用同一設備。

(三)擁有一套網路及軟硬體備援系統，可以執行營運數位簽章系統異常時之備援與

系統回復。

(四)營運之電腦機房及相關設備須設置國內，以利主管機關查核。

四、憑證機構之作業制度

(一)對於憑證紀錄保存期限於保險契約期滿或終止後至少五年。

(二)對憑證資料應妥善保管並負保密之責。

(三)禁止委託其他機構代為處理數位簽章業務。

五、憑證機構之內部稽核與控管

(一)全部憑證作業，由實體設備的操作到憑證作業系統的執行，皆須確實留存相關作業文件及稽核紀錄。

(二)除了管理與作業人員外，並設置安控稽核部門及稽核人員，負責查核相關業務。

第五章　契約範本

第十七條

保險業與消費者約定以電子文件方式簽發保險單或暫保單，應本公平合理、平等互惠及誠信原則。

第六章 附則

第十八條

為因應資訊技術之發展與進步，保險業應定期審視本自律規範內容進行調整修正。

第十九條

本自律規範由中華民國人壽保險商業同業公會與中華民國產物保險商業同業公會共同訂定，經各該公會理事會通過，並報請主管機關備查後實施；修正時亦同。