

保險業透過「金融行動身分識別（金融Fast-ID）」辦理資料共享自律

規範訂定說明對照表

6/6 呈報草案條文	8/14 會議後呈報草案條文	訂定說明
<p>第一條</p> <p>為使保險業偕同所屬金融控股公司（以下簡稱金控）或其所屬之金融機構子公司（以下簡稱偕同合作公司），透過「金融行動身分識別（金融FIDO）」辦理資料共享暨身分認證授權作業（以下稱本業務）有一致性之規範，以提升保戶使用金融服務之安全性、便利性及效率，保障消費者權益，特訂定本自律規範。</p>	<p>第 1 條</p> <p>為使保險業偕同所屬金融控股公司之金融機構子公司（以下簡稱偕同合作公司），透過「金融行動身分識別（金融Fast-ID）」辦理資料共享（以下稱本業務）有一致性之規範，以提升保戶使用金融服務之安全性、便利性及效率，保障消費者權益，特訂定本自律規範。</p>	<ol style="list-style-type: none"> 1. 說明規範目的和定義此規範適用範圍公司。 2. 因應金融FIDO正式名稱進行修正
<p>第二條</p> <p>保險業辦理本業務，應遵循保險法、消費者保護法、金融消費者保護法、個人資料保護法、電子簽章法、保險業內部控制及稽核制度實施辦法、保險業辦理電子商務應注意事項、金融機構間資料共享指引、金融機構辦理快速身分識別機制安全控管作業指引、保險業經營電子商務自律規範及保險業辦理資訊安全防護自律規範等相關法令及自律規範之規定。</p>	<p>第 2 條</p> <p>保險業辦理本業務，應遵循保險法、消費者保護法、金融消費者保護法、個人資料保護法、電子簽章法、保險業內部控制及稽核制度實施辦法、保險業辦理電子商務應注意事項、金融機構間資料共享指引、金融機構辦理快速身分識別機制安全控管作業指引、保險業經營電子商務自律規範及保險業辦理資訊安全防護自律規範等相關法令及自律規範之規定。</p>	<p>列舉和此規範有關之既有法規、指引、注意事項等。</p>
<p>第三條</p> <p>本業務係指保險業提供客戶透過金控或偕同合作公司建置之「金融行動身分識別平臺」（以下簡稱金融FIDO平臺）進行身分認證並：</p> <p>一、於註冊保險業之網路會員時，自動帶入客戶基本資料及其他經客戶及合作金融機構同意</p>	<p>第 3 條</p> <p>本業務係指保險業提供客戶透過偕同合作公司建置之「金融行動身分識別平臺」（以下簡稱金融Fast-ID平臺）進行身分認證，並得共享下列資料：</p> <p>一、於註冊保險業之網路會員時，經客戶及偕同合作公司同意，自動帶入客戶基本資料。</p>	<ol style="list-style-type: none"> 1. 說明此規範之應用場景及服務內容。 2. 因應金融FIDO正式名稱進行修正 3. 修正語句邏輯順序

<p>共享之資料。</p> <p>二、於保險業或偕同合作公司之行動應用程式（APP）完成授權作業後，申請資產總覽查詢服務。</p>	<p>二、於保險業或偕同合作公司之行動應用程式（APP）完成授權作業後，申請資產總覽查詢服務。</p>	
<p>第四條</p> <p>前條第一項第二款之資產總覽查詢服務係提供保險業既有保戶透過保險業或協同合作公司之行動應用程式（APP），查詢保單及其他偕同合作公司之資產及相關資訊。</p>	<p>第 4 條</p> <p>前條第一項第二款之資產總覽查詢服務係提供保險業既有保戶透過保險業或偕同合作公司之行動應用程式（APP），得線上查詢保險契約內容及其他偕同合作公司之資產及相關資訊。</p>	<ol style="list-style-type: none"> 1. 定義資產總覽查詢服務之資料範圍。 2. 同電子商務應注意事項的說明，得線上查詢保險契約內容。
<p>第五條</p> <p>本業務提供對象以具完全行為能力，且已於金融 FIDO 平臺完成註冊及身分認證作業之客戶為限。</p> <p>客戶首次申請資產總覽查詢服務前，須依保險業或偕同合作公司之行動應用程式（APP）指定方式登入後，點選同意所載法定相關告知事項，包括但不限於審閱個人資料蒐集處理利用告知事項、資料共享契約、相關服務授權等，始得申請。</p> <p>保險業提供資產總覽查詢服務前，須確認客戶授權之有效性，並留存其授權紀錄以提供查核。</p>	<p>第 5 條</p> <p>本業務提供對象以具完全行為能力，且已於金融 Fast-ID 平臺完成註冊及身分認證作業之客戶為限。</p> <p>客戶首次申請資產總覽查詢服務前，須依保險業或偕同合作公司之行動應用程式（APP）指定方式登入後，點選同意所載法定相關告知事項，包括但不限於個人資料蒐集處理利用告知事項、資料共享契約、相關服務授權等，始得申請。</p> <p>保險業提供資產總覽查詢服務前，須確認客戶授權之有效性，並留存其授權紀錄以提供查核。</p>	<ol style="list-style-type: none"> 1. 說明此應用場景及服務提供前之相關告知事項、申請人條件。 2. 因應金融 FIDO 正式名稱進行修正
<p>第六條</p> <p>保險業與偕同合作公司所建立本業務之合作關係，應依金融機構間資料共享指引第七點第一項第四款規定辦理。</p> <p>保險業對本業務應建立資通安全事件通報程序，遇個人資料外洩或相關資安事件而有影響本業務時，除依前開通報程序辦理</p>	<p>第 6 條</p> <p>保險業與偕同合作公司所建立本業務之合作關係，應依金融機構間資料共享指引第七點第一項第四款規定辦理。</p> <p>保險業對本業務應建立資通安全事件通報程序，遇個人資料外洩或相關資安事件而有影響本業務時，除依前開通報程序辦理</p>	<p>說明保險業與偕同合作公司間應建立之合作關係與資安事件處理機制。</p>

<p>外，應即另行通知偕同合作公司。</p>	<p>外，應即另行通知偕同合作公司。</p>	
<p>第七條</p> <p>保險業辦理本業務，應取得資訊安全管理系統國際標準認證（ISO27001）、個人資料管理系統（PIMS）之認證，針對所傳輸之個人資料應建置適當之保護設備或技術，並採取適當之存取管制。</p> <p>保險業與偕同合作公司應留存與本業務相關之申請紀錄、個人資料傳輸、客戶與系統管理者操作軌跡及 API 執行認證紀錄等資訊，並依主管機關資訊安全防護相關法令及本會相關自律規範規定辦理。</p> <p>前項操作軌跡應自 API 執行認證紀錄存取日起保存五年。</p>	<p>第 7 條</p> <p>保險業辦理本業務，保險業及偕同合作公司應取得資訊安全管理系統國際標準認證（ISO27001）、個人資料管理系統（PIMS）之認證，針對所傳輸之個人資料應建置適當之保護設備或技術，並採取適當之存取管制。</p> <p>保險業與偕同合作公司應留存與本業務相關之申請紀錄、個人資料傳輸、客戶與系統管理者操作軌跡及 API 執行認證紀錄等資訊，並依主管機關資訊安全防護相關法令及本會相關自律規範規定辦理。</p> <p>前項操作軌跡應自 API 執行認證紀錄存取日起保存五年，倘若因處理申訴、調解及訴訟等程序，而有繼續處理及利用前開個人資料之需求者，得續予保存至該等爭議處理終結之日起一年。</p>	<ol style="list-style-type: none"> 1. 說明保險業與偕同合作公司間應具備之資訊條件以及軌跡留存、處理機制。 2. 增加軌跡保存年限例外處理規則
<p>第八條</p> <p>保險業應將本業務之人員管理、資料傳輸過程、資訊交換作業、資料儲存作業、紀錄保存及爭議處理機制等安全控管機制，納入保險業內部控制及稽核項目，並每年至少辦理一次自行查核。</p>	<p>第 8 條</p> <p>保險業應將本業務之人員管理、資料傳輸過程、資訊交換作業、資料儲存作業、紀錄保存及爭議處理機制等安全控管機制，納入保險業內部控制及稽核項目，內部稽核單位並應每年至少辦理一次查核。</p> <p>保險業違反本自律規範經查核屬實者，提報各該公會理監事會，處以新臺幣 5 萬元以上，新臺幣 20 萬元以下之罰款；前述處理情形並應於 1 個月內報主管機關。</p>	<ol style="list-style-type: none"> 1. 說明辦理此業務應進行的內稽內控項目 2. 訂定相關罰款內容。

<p>第九條</p> <p>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（監）事會決議通過，報主管機關備查後施行，修正時亦同。</p>	<p>第 9 條</p> <p>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（監）事會決議通過，報主管機關備查後施行，修正時亦同。</p>	<p>說明此規範後續調整所需之程序。</p>
---	---	------------------------