柏文健康事業股份有限公司
個人資料保護管理內部控制制度
會計師專案審查確信報告
民國112年1月1日至113年3月31日

目　　錄

安永聯合會計師事務所

80052 高雄市中正三路2號17樓
17F, No. 2, Zhongzheng 3rd Road
Kaohsiung City, Taiwan, R.O.C.

Tel: 886 7 238 0011
Fax: 886 7 237 0198
www.ey.com/taiwan

會計師合理確信報告

柏文健康事業股份有限公司公鑒：

柏文健康事業股份有限公司（以下簡稱　貴公司）對民國 112 年 1 月 1 日至 113 年 3 月 31 日旗下「健身工廠」會員個人資料保護內部控制制度之設計及執行情形所出具之聲明書，業經本會計師執行必要程序竣事。

確信標的資訊與適用基準

本確信案件之標的資訊係　貴公司對民國 112 年 1 月 1 日至 113 年 3 月 31 日「健身工廠」會員個人資料保護內部控制制度之設計及執行之聲明書（以下稱「標的資訊」），詳附件。

用以衡量或評估上開標的資訊之適用基準係「個人資料保護法」、「個人資料保護法施行細則」以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。

先天限制

由於確信工作係採抽樣方式進行，任何個人資料保護管理之內部控制制度均有其先天上之限制，故未必能查出所有業已存在之重大不實表達，無論導因於舞弊或錯誤。

管理階層之責任

管理階層之責任係依據個人資料保護相關法令與指引建立內部控制制度，且隨時檢討，以維持內部控制制度之設計及執行持續有效，並於評估其有效性後，據以出具內部控制制度聲明書。

會計師之責任

本會計師之責任係依據所取得之證據對標的資訊作成結論。

本會計師依照財團法人中華民國會計研究發展基金會所發布之確信準則 3000 號「非屬歷史性財務資訊查核或核閱之確信案件」對確信標的執行必要程序以取得合理確信，並對確信標的在所有重大方面是否遵循適用基準及是否允當表達表示結論。

EY安永
Building a better working world

獨立性及品質管理規範

本會計師及所隸屬會計師事務所已遵循會計師職業道德規範中有關獨立性及其他道德規範之規定，該規範之基本原則為正直、公正客觀、專業能力及專業上應有之注意、保密及專業行為。 此外，本會計師所隸屬會計師事務所遵循品質管理準則第1號「會計師事務所之品質管理」之規範，維持完備之品質管理制度，包含與遵循職業道德規範、專業準則及所適用法令相關之書面政策及程序。

所執行程序之彙總說明

本會計師係基於專業判斷規劃及執行必要程序，以獲取相關確信標的之證據。所執行之程序包括瞭解公司內部控制制度、評估管理階層評估整體內部控制制度有效性之過程、測試及評估其與外部財務報導及保障資產安全有關之內部控制制度設計及執行之有效性，以及本會計師認為必要之其他審查程序。本會計師相信此項審查工作可對所表示之結論提供合理之依據。

確信結論

依本會計師意見，依照「個人資料保護法」、「個人資料保護法施行細則」以及「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」之內部控制制度有效性判斷項目判斷，柏文健康事業股份有限公司旗下「健身工廠」會員個人資料保護內部控制制度於民國112年1月1日至民國113年3月31日之設計及執行，在所有重大方面可維持有效性；柏文健康事業股份有限公司於民國113年5月28日所出具謂經評估其旗下「健身工廠」會員個人資料保護內部控制制度係有效設計及執行之聲明書，在所有重大方面則屬允當。

與案件特定層面有關之發現

如柏文健康事業股份有限公司內部控制制度聲明書第六款所述， 貴公司於本專案審查特定範圍於審查期間(民國112年1月1日至民國113年3月31日)內曾有部分缺失，惟該等缺失並非屬重大缺失或已由 貴公司於審查期間內完成改善，本會計師之結論未因該等事項而修正。

其他事項

本確信報告出具後，本會計師不負更新本確信報告之責任。

EY安永
Building a better working world

使用限制

本確信報告僅供　貴公司申報主管機關使用或及其監理使用，不得作為其他用途或分送其他人士。

安永聯合會計師事務所

會計師：陳 政 初

地址：高雄市新興區中正三路2號17樓
中華民國 113 年 5 月 31 日

柏文健康事業股份有限公司
資通安全管理內部控制制度
會計師專案審查確信報告
民國112年1月1日至113年3月31日

目　　錄

安永聯合會計師事務所

80052 高雄市中正三路2號17樓
17F, No. 2, Zhongzheng 3rd Road
Kaohsiung City, Taiwan, R.O.C.

Tel: 886 7 238 0011
Fax: 886 7 237 0198
www.ey.com/taiwan

會計師有限確信報告

柏文健康事業股份有限公司公鑒：

柏文健康事業股份有限公司（以下簡稱　貴公司）對民國 112 年 1 月 1 日至 113 年 3 月 31 日旗下「健身工廠」會員個人資料關聯系統機敏性資料處理（含連線管理與委外管理）之資通安全管理內部控制制度之設計及執行情形所出具之聲明書，業經本會計師執行必要程序竣事。

確信標的資訊與適用基準

本確信案件之標的資訊係　貴公司對民國 112 年 1 月 1 日至 113 年 3 月 31 日「健身工廠」會員個人資料關聯系統機敏性資料處理（含連線管理與委外管理）之資通安全管理（以下稱「標的資通安全管理」）之內部控制制度之設計及執行之聲明書（以下稱「標的資訊」），詳附件。

用以衡量或評估上開標的資訊之適用基準係「上市上櫃公司資通安全管控指引」。

先天限制

由於確信工作係採抽樣方式進行，任何資通安全管理內部控制制度均有其先天上之限制，故未必能查出所有業已存在之重大不實表達，無論導因於舞弊或錯誤。

管理階層之責任

管理階層之責任係依據資通安全管理相關法令與指引建立內部控制制度，且隨時檢討，以維持內部控制制度之設計及執行，以確保標的資訊未存有導因於舞弊或錯誤之重大不實表達。

會計師之責任

本會計師之責任係依據所取得之證據對標的資訊作成結論。

本會計師依照財團法人中華民國會計研究發展基金會所發布之確信準則 3000 號「非屬歷史性財務資訊查核或核閱之確信案件」之要求規劃並執行有限確信工作，以對標的資訊是否存有重大不實表達出具有限確信報告。本會計師依據專業判斷，包括對導因於舞弊或錯誤之重大不實表達風險之評估，以決定確信程序之性質、時間及範圍。

本會計師相信已取得足夠及適切之證據，以作為表示有限確信結論之基礎。

EY安永
Building a better working world

獨立性及品質管理規範

本會計師及所隸屬會計師事務所已遵循會計師職業道德規範中有關獨立性及其他道德規範之規定，該規範之基本原則為正直、公正客觀、專業能力及專業上應有之注意、保密及專業行為。 此外，本會計師所隸屬會計師事務所遵循品質管理準則第1號「會計師事務所之品質管理」之規範，維持完備之品質管理制度，包含與遵循職業道德規範、專業準則及所適用法令相關之書面政策及程序。

所執行程序之彙總說明

有限確信案件中執行程序之性質及時間與適用於合理確信案件不同，其範圍較小，因此，有限確信案件中取得之確信程度明顯低於合理確信案件中取得者。本會計師所設計之程序係為取得有限確信並據此作成結論，並不提供合理確信必要之所有證據。

儘管本會計師於決定確信程序之性質及範圍時曾考量 貴公司內部控制之有效性，惟本確信案件並非對 貴公司整體內部控制之有效性表示意見。

有限確信案件包括進行查詢，主要係對負責標的資訊及相關資訊之人員進行查詢及其他適當程序。

本會計師係基於專業判斷規劃及執行必要程序，以獲取相關標的資訊之證據，本會計師所執行之程序包括：

- 與 貴公司人員進行訪談，瞭解 貴公司標的資通安全管理環境及風險；
- 透過獲取與檢視資通安全作業程序，以瞭解 貴公司標的資通安全管理防護措施；並透過實地檢查系統防火牆與端點加密設定畫面評估標的資通安全管理連線設定防護措施；
- 透過詢問與檢查標的資通安全管理之外部檢測文件，以瞭解 貴公司標的資通安全管理之資安風險評估；並透過審查應用系統弱點掃描與行動應用APP基本資安檢測評估標的資通安全管理之資安風險評估；
- 透過取得與檢視資訊作業委外安全管理程序，以瞭解 貴公司標的資通安全管理之委外管理措施；並透過審查委外廠商合約內容與管理程序評估標的資通安全管理之委外管理程序；
- 透過檢查標的資通安全管理之管理辦法，以瞭解 貴公司標的資通安全管理持續改善機制；檢查內部控制制度是否已依據適用基準中概述的方法執行管理。

結論

依據所執行之程序及所取得之證據，本會計師未發現標的資訊有未依照適用基準出具而須作重大修正之情事。

EY安永
Building a better working world

與案件特定層面有關之發現

本會計師執行確信過程中，發現　貴公司於本專案審查特定範圍內部控制制度設計與執行方面，於審查期間(民國 112 年 1 月 1 日至民國 113 年 3 月 31 日)內曾有部分缺失，惟該等缺失並非屬重大缺失或已由　貴公司於審查期間內完成改善，本會計師之結論未因該等事項而修正。

其他事項

本確信報告出具後，本會計師不負更新本確信報告之責任。

使用限制

本確信報告僅供　貴公司申報主管機關使用或及其監理使用，不得作為其他用途或分送其他人士。

安永聯合會計師事務所

會計師：陳 政 初

地址：高雄市新興區中正三路2號17樓
中華民國 113 年 5 月 31 日

柏文健康事業股份有限公司

內部控制制度聲明書

日期：民國113年5月28日

本公司民國112年1月1日至113年3月31日止會員個人資料保護管理及會員個人資料關聯系統機敏性資料處理(含連線管理與委外管理)之資通安全管理(以下稱「會員個人資料關聯系統之資通安全管理」)內部控制制度，依據自行評估的結果，謹聲明如下：

一、本公司確知建立、實施和維護會員個人資料保護管理及會員個人資料關聯系統之資通安全管理內部控制制度係本公司董事會及經理人之責任，本公司業已建立此一制度。其目的係在對個人資料保護以及資通安全相關法令規章之遵循目標的達成，提供合理的確保。

二、內部控制制度有其先天限制，不論設計如何完善，有效之內部控制制度亦僅能對上述目標之達成提供合理的確保；而且，由於環境、情況之改變，內部控制制度之有效性可能隨之改變。惟本公司之內部控制制度設有自我監督之機制，缺失一經辨認，本公司即採取更正之行動。

三、本公司係依據「個人資料保護法」、「個人資料保護法施行細則」及「上市上櫃公司資通安全管控指引」之相關規定，定期評估確認所保有之個人資料狀況，界定之個人資料範圍及其業務涉及個人資料蒐集、處理、利用之流程，評估可能產生之個人資料保護風險，以及定期檢視公司之核心業務及應保護之機敏性資料，確保機密性、完整性及可用性，並鑑別資通系統或資訊可能遭遇之資通安全風險，並根據風險評估之結果，訂定適當之管理機制，並負責設計、建置及維護有效之內控控制機制。

四、本公司業已完成上開會員個人資料保護管理及會員個人資料關聯系統之資通安全管理內部控制制度設計及執行有效性之評估，並依該評估結果，認為本公司於民國112年1月1日至113年3月31日止會員個人資料保護管理及會員個人資料關聯系統之資通安全管理內部控制制度之設計及執行，如第六段函文說明所述之會員個資外洩及資安疑慮，本公司已於評估期間及民國113年5月28日前執行相關行動及改善措施，係屬有效，其能合理確保上述目標之達成。

五、本公司應遵行之法令規章不以前開所聲明者為限。

六、依據臺灣證券交易所股份有限公司民國113年2月7日臺證上一字第1130002035號函，有關本公司旗下「健身工廠」會員個資外洩及資安疑慮，函請本公司委託非簽證會計師執行民國112年1月1日至113年3月31日止旗下「健身工廠」會員個人資料保護管理及資通安全管理等2項內部控制制度專案審查，就審查期間之發現及臺灣證券交易所股份有限公司函文說明缺失事項，本公司於民國113年5月28日前已執行相關行動及改善措施，相關內容詳本聲明書附件。

七、本聲明書將成為本公司年報及公開說明書之主要內容，並對外公開。上述公開之內容如有虛偽、隱匿等不法情事，將涉及證券交易法第二十條、第三十二條、第一百七十一條及第一百七十四條等之法律責任。

八、本聲明書業經本公司民國113年5月28日董事會通過，出席董事七人中，無人持反對意見，均同意本聲明書之內容，併此聲明。

柏文健康事業股份有限公司

董事長：陳尚義 簽章

總經理：林洵賢 簽章

聲明書附件

應加強事項	改善措施	預定完成時間
一、 公司發生個資外洩事件，證交所於113年1月16日來文，有以下事項		
(一)、應以最小化原則蒐集、處理及利用個人資料，建議重新檢視資通系統存取架構，僅存放必要之個人資料，開放外部系統介接存取時應使用api或view等方式，僅提供所需個人資料	公司已透過防火牆資訊傳輸流量監控以達最小化蒐集、處理及利用個人資料之目的。	已於112年11月18日完成改善
(二)、建議具備存放及存取個人資料功能之系統(包含委外維運管理系統)皆應強化端點防護機制	111年度陸續完成端點防護強化 (1) 111/9/1- 新版防火牆上線-Antivirus，IPS&IDS防護設定(威脅偵測防護，漏洞防護)，黑白名單IP啟用 (2) 111/10/1- 廠館防火牆-限定網路應用程式 (禁制非法Application存取，包含Line/Dropbox/Gmail/Google-Drive等網路行為)。 (3) 112/2/1- 總公司防火牆-限定網路應用程式 (禁制非法Application存取，包含Line/Dropbox/Gmail/Google-Drive等網路行為)。 (4) 112/1/1~112/6/30-端點強化-設定端點固定IP (各單位端點設備增列固定IP管制，非內部合規IP，無法取得內網服務)。 (5) 112/11/1-端點防護-限制儲存媒介 (禁制端點管制行為，同時增列1年以上log調閱基礎)。 (6) 113/3/1-端點防護-文件檔案加密 (企業內部各類文檔統一進行加密行為)。	如左列所示時間，已完成改善
(三)、核心系統應建立網頁應用程式防火牆、入侵偵測防禦系統等相關防護機制；	(1) WAF檢測及SOC等資通安全補強，113年度，已委由外部資安團隊，透過弱點掃描、滲透測試等資安健診服務，進行重要系統審視及改善補強。 (2) 114年度起，將持續委託外部資安團隊，於各主機系統增列及重大系統版本更新時，進行相關資安檢測服務之改善補強。	(1) 預計於113年9月完成改善 (2) 預計於114年完成改善
(四)、建議應定期針對所有對外服務系統(含委外維運管理系統)辦理應用系統弱點掃描及滲透測試；與個人資料相關之APP應送交「行動應用App基本資安檢測」	(1) 已委請外部廠家進行弱點掃描及滲透測試等服務，已於113/5/10 完成會員相關平台初測。 (2) 我的健身工廠 App (iOS & Android) 已於113/4/22完成檢測並通過安全等級L3。	(1) 已於113年5月10日前完成改善 (2) 已於113年4月22日完成改善
二、公司針對個資保護與資通安全需予加強有以下事項		
(一)、查核期間未重新盤點個人資料範圍與進行個人資料隱私風險評估	盤點個人資料範圍已於113年5月2日完成，個人資料隱私風險評估搭配ISO 27001/27701 專案進行中，已於113年5月17日完成。	已於113年5月17日完成改善
(二)、查核期間未明確設定特定目的消失或期限屆滿時刪除個人資料	盤點個人資料範圍已於113年5月2日完成，並已於113/5/17進行目的消失或期限屆滿時之文件進行銷毀，並於113/5/20完成銷毀。	已於113年5月17日完成改善
(三)、查核期間未執行自我評估個人資料安全維護	個資小組已完成自我評估個人資料安全維護。	已於113年5月13日完成改善
(四)、查核期間未執行個人資料事故演練	已於113年5月17日進行演練。	已於113年5月17日完成改善

應加強事項	改善措施	預定完成時間
(五)、部分分廠之個人資料之紙本文件與平板未存放於上鎖櫃子且部分分廠未明顯劃分管制區域	已於113/5/14發布個資保護公告予公司全體同仁並與各分廠溝通教練部管制標語，加強管制各分廠保有個人資料之紙本文件及授權使用之可攜式儲存媒體，並劃分管制區域。	已於113年5月14日完成改善
(六)、查核期間未執行委外廠商稽核。	已於113年5月17日提供廠商個資安全管理措施自評表，另完整委外廠商稽核作業待配合ISO27001/27701專案執行。	已於113年5月17日提供廠商個資安全管理措施自評表，另完整委外廠商稽核作業預計113年12月底前完成改善
(七)、Cofit資訊合約查核期間內容並未包含資安要求及對委外廠商資安稽核權	(1) 本公司於112年事故發生後，即重新審視合約內容，未簽立完整保密協定義務之廠商，已重新擬定補充文件給與廠商進行補簽。新簽立合約亦將保密協定文件列為獨立簽立之合約內容。 (2) Cofit目前與柏文簽定合約，只針對後續運營等模式進行約束，與資安相關部分早已在案發重新擬定委外廠商之合約，並寄送給Cofit並取得回簽資料。	已於113/5/21取得 Cofit簽回之委外廠商個人資料保護承諾書。
(八)、查核期間未執行弱點掃描、滲透測試及源碼掃描安全檢測並評估資訊風險	已委請外部廠家進行弱點掃描及滲透測試等服務，已於113/5/7完成會員相關平台初測。	已於113年5月7日完成改善
(九)、BI應用系統與APP密碼原則設定未臻完善	(1) 預計於113/Q4前完成新版BI工具之評選，並於114年度導入；廠商評估條件必須以AD帳套結合，未來平台皆以個人AD帳套登入並針對職級角色作為權限配置之基礎。 (2) 預計113年Q2完成APP密碼原則修正。	(1) 113/Q4前 (2) 113/Q2前