企業法規符合性自我檢核評估表

公司：

自評部門

職稱：

歐盟一般資料保護規則（General Data Protection Regulation，GDPR）於 2018 年 5 月 25 日正式施行，該規則對我國與歐盟（含冰島、列支敦士登及挪威）有商務往來之企業，於個人資料保護及傳輸等遵法措施上可能造成衝擊。有鑑於此，企業法規符合性自我檢核評估表（以下簡稱本表）將提供企業做為蒐集、處理或利用個人資料時之自我檢核依據，協助企業檢視其法規遵循情形，引導業者建立自主之個人資料保護與管理機制。

填表說明：

- 本表係依據歐盟 GDPR 之規定，依序展開個人資料保護與管理之基礎措施與建議，業者可參考本表，但不以此為限，以考量業者營運風險與需求，訂定符合業者本身營運需求之個人資料保護與管理制度。
- 另，提醒您如貴公司為歐盟企業之供應商或承包商，而有為其蒐集、處理或利用個人資料之情形，仍應注意 GDPR 之規定。
- 本表供貴公司為初步之自我評估，貴公司仍宜遵循 GDPR 之規定，落實相關規範要求。

開始自我評估，GO！

類別	查核項目	補充說明	自評結果	執行困難
適用性	1. 公司是否於**歐盟境內設有分支機構，並有進行個人資料蒐集、處理或處理之相關行為**？	分支機構指分公司、子公司、聯絡處或辦事處等。§§2、3	☐ 是 ☐ 否 ☐ 其他_____	說明：

類別	查核項目	補充說明	自評結果	執行困難
	2. 若未於歐盟境內設立分支機構，公司是否向**歐盟境內之人民提供商品或服務**（無論是否須付費）？	商品或服務如： 1.產品服務提到歐盟成員國名稱。 2.於歐盟境內有廣告或行銷。 3.於搜尋引擎購買廣告促使歐盟消費者知悉。 4.經營活動具國際性、商品或服務使用歐盟之語言或貨幣。 5.於歐盟境內提供運送商品服務。 6.最高層級網域名稱為歐盟境內網域名稱。 §§2、3	☐ 是 ☐ 否 ☐ 其他_____	說明：
	3. 若未於歐盟境內設立分支機構，公司是否**對歐盟境內之人民於歐盟內進行行為監控**？	監控如：透過網路分析或預測使用者之使用習慣、喜好或建檔等，例如販售具有電子定位系統商品或對個人健康狀態進行紀錄。§§2、3	☐ 是 ☐ 否 ☐ 其他_____	說明：
同意之有效性	4. 公司是否以**簡潔、透明、易懂、方便取得之格式、簡易之語言**等適當方式或措施，提供當事人**行使權利之管道，並告知、提供當事人蒐集其個人資料之相關資訊**？	該資訊包含：資料蒐集、處理及利用之類型、目的、法律依據、公司名稱、聯繫方式等。§12	☐ 是 ☐ 否 ☐ 其他_____	說明：
	5. 公司向當事人蒐集個人資料時，是否以**易懂、方便取得之格式、簡易之語言，取得當事人之同意**？	§7	☐ 是 ☐ 否 ☐ 其他_____	說明：
	6. 公司**徵求當事人同意的項目是否很醒目**，並與契約中之條款、條件做**區隔**？	§7	☐ 是 ☐ 否 ☐ 其他_____	說明：
	7. 公司是否告知當事人**可以隨時撤銷其同意？撤銷方**	§7	☐ 是 ☐ 否	說明：

類別	查核項目	補充說明	自評結果	執行困難
	式是否與同意一樣以**易懂、方便取得之格式、簡易之語言為之**？		☐ 其他_____	
	8. 當公司向**未滿16歲**之人提供資訊社會服務（社交媒體、網站）時，是否**事前獲得父母或監護人**的同意？	§8	☐ 是 ☐ 否 ☐ 其他_____	說明：
當事人權益之強化	9. 接近使用權：公司是否訂有當事人**申請接近使用**其個人資料之方式或因應措施？	當事人有權向貴公司確認是否正在處理自己之個資，且可以接近使用其個資及相關資訊(如個資使用目的及種類、個資將被儲存的期間（如不能確定，則提供確定該期間的相關準則）、自動化決策（包括建檔）的存在、個資被披露的接受者等）。§15	☐ 是 ☐ 否 ☐ 其他_____	說明：
	10. 更正權：公司是否訂有當事人**請求更正**其個人資料之方式或因應措施？	§16	☐ 是 ☐ 否 ☐ 其他_____	說明：
	11. 刪除權(1)：公司是否訂有**當事人請求刪除**其個人資料之方式或因應措施？	§17	☐ 是 ☐ 否 ☐ 其他_____	說明： ：
	12. 刪除權(2)：公司是否訂有相關措施，於當事人行使刪除權時，在**合理範圍內通知其他處理該當事人個資之控管者**？	§17	☐ 是 ☐ 否 ☐ 其他_____	說明：
	13. 限制處理權：公司是否讓當事人得以簡便之方式**請求停止處理其個人資料**？	請求停止使用之情況：對資料使用的合法性、正確性等具有爭議，當事人得請求停止使用。§18	☐ 是 ☐ 否 ☐ 其他_____	說明：
	14. 通知義務：當個人資料已經被傳遞給其他控制者的	§19	☐ 是 ☐ 否	說明：

類別	查核項目	補充說明	自評結果	執行困難
	情況下，公司是否訂有針對當事人提出**更正、刪除或限制處理之請求時**，在合理範圍內通知其傳遞對象之因應措施？		☐ 其他_____	
	15. 資料可攜權：公司是否訂有當事人**行使資料可攜權**之因應措施，使當事人得以完整的以一般使用、機器可讀之方式，提供其個人資料予其他資料控管者？	§20	☐ 是 ☐ 否 ☐ 其他_____	說明：
	16. 拒絕權：公司是否訂有當事人**提出拒絕資料蒐集、處理、利用請求**時之因應措施？	§21	☐ 是 ☐ 否 ☐ 其他_____	說明：
	17. 公司的客戶是否得以簡便之方式反對可能會影響到他們的分析或自動化做成之決策？	自動化處理程序，以個資做基礎，評量某人的各種特徵。例如線上汽車保險業務，透過演算法自動決定用戶的保費金額。§22	☐ 是 ☐ 否 ☐ 其他_____	說明：
資料安全性	18. 公司是否依據蒐集、處理或利用個人資料**所可能產生之風險**，採取適當之**安全維護措施**，以確保個人資料之**風險程度維持適當之安全水準**？	安全維護措施如： 1. 個資假名化、加密。 2. 資料處理系統有效運作。 3. 個資受破壞有回復能力。 4. 定期檢測資料處理科技的有效性。 §32	☐ 是 ☐ 否 ☐ 其他_____	說明：
	19. 公司是否訂有個人**資料發生侵害時向監管機關通報或通知當事人之通報措施或方式？**	個資侵害發生時，應於 72 小時內通知主管機關，如高度影響當事人權益時應即時通知當事人。 §§33、34	☐ 是 ☐ 否 ☐ 其他_____	說明：
	20. 公司如為個人資料**處理者**，是否訂定發生資料侵	§§33、34	☐ 是 ☐ 否	說明：

類別	查核項目	補充說明	自評結果	執行困難
	害事件時，即時通知控管者之方式或因應措施？		☐ 其他_____	
	21.公司是否制訂資料保護衝擊評估程序？	3 種情形須進行評估： 1. 基於個人資料之自動化蒐集或利用大規模分析，做成一定結果。 2. 大規模蒐集、處理或利用設涉及前科之資料。 3. 大規模且系統性監控公眾場所。 §35	☐ 是 ☐ 否 ☐ 其他_____	說明：
	22. 公司是否訂有與個人資料蒐集、處理或利用相關之文件管理保存措施，並保存 GDPR 第 30 條所要求及相關之各項紀錄？	紀錄包含公司聯絡方式、資料處理目的、個人資料類別、資料揭露或傳輸之對象等。§30	☐ 是 ☐ 否 ☐ 其他_____	說明：
	23.公司是否確認蒐集、處理、利用特種個資時，有 GDPR 第 9、10 條所定之合法事由，並採取適當安全措施維護安全？	合法事由包含:獲得當事人同意或自行公開之個人資料、履行法律義務、有重大利益所為必要之處理、由歐盟機關授權處理等。 §§9、10	☐ 是 ☐ 否 ☐ 其他_____	說明：
責問與治理機制	24.公司如未於歐盟設立據點，是否以書面指定歐盟境內代表？且其代表是否有權代表其處理與蒐集、處理、利用個人資料有關之議題？	該境內代表由律師事務所、顧問公司、私人企業擔任均可。§27	☐ 是 ☐ 否 ☐ 其他_____	說明：
	25.公司是否有設置個人資料保護員 (Data Protection Officer)，並確保其能獨立行使其職權、向最高層報告業務之執行情形，並能涉入與個資保護有關之業務？	需要設置 DPO 之三種情形 ： 1.除法院行使其司法權外，該處理係由公務機關或機構執行。 2.控管者或處理者之核心活動，依其本質、範圍或目的，需要定期且系統性大規模監控資料主體。	☐ 是 ☐ 否 ☐ 其他_____	說明：

類別	查核項目	補充說明	自評結果	執行困難
		3.控管者或處理者之核心活動,包括大規模處理特殊類型之資料(如揭露種族或人種、政治意見、宗教或哲學信仰或貿易聯盟會員之個人資料、以及基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與自然人之性生活或性傾向)及前科與犯罪相關之個人資料。§37		
跨境傳輸	26.公司如於歐盟境內設立據點時，其進行跨境傳輸之目的地是否為歐盟所公告，具有充足保護程度之國家？	目前公告國家：安道爾、阿根廷、加拿大(商業組織)，法羅群島、根西島、以色列、馬恩島、日本、澤西島、新西蘭、瑞士、烏拉圭和美國（僅限於隱私防護組織)。§45	☐ 是 ☐ 否 ☐ 其他_____	說明：
	27.當公司跨境傳輸之目的地非上述公告國家，公司是否能採取一定措施為適當保護？	保護措施如： 1. 僅於同一集團內傳輸時，制定經主管機關核准之企業自我拘束規則。 2. 與所有傳輸對象簽屬主管機關或執委會核准之標準契約條款。 §§40、42、46、47、93	☐ 是 ☐ 否 ☐ 其他_____	說明：
	28.當公司如不能依上述方法進行跨境傳輸時，該傳輸是否是屬必須之情況下，且符合下列要件之一： (1)在告知當事人可能風險後，取得當事人之明確同意。 (2)履行資料當事人與公司間契約、應當事人要求執行契約前措施、公司與第	§49	☐ 是 ☐ 否 ☐ 其他_____	說明：

類別	查核項目	補充說明	自評結果	執行困難
	三方履行或締結基於當事人利益之契約。 (3)有重要公共利益。 (4)建構、行使或防禦法律上之請求。 (5)保護當事人重要利益且法律上或實際上無法取得當事人同意。 (6)歐盟或會員國法律所規定之資料公開等需求。			

<u>諮詢服務</u>

聯絡方式：

諮詢內容：

有任何問題歡迎 MAIL 回傳，將有專人協助回覆，謝謝！

負責人：林玉書 研究員

聯絡電子信箱：<yuslin@iii.org.tw>