

委外單位個人資料保護檢查表

Personal Data Protection Checklist for Outsourced Contractors

委外專案受託單位個人資料保護檢查表 Personal Data Protection Checklist for Outsourced Contractors	
☐ 自評 Self-assessment ☐ 查核 Audit	
專案名稱 (契約編號) Project name (contract no.)	
委外單位名稱 Name of outsourced contractor	
蒐集、處理及利用之個人資料 Personal data collected, processed, and used	
自評／查核人員 Self-assessor / Auditor	
自評／查核日期 Date of self-assessment / audit	

項次 No.			查核項目 Audit item	符合 Compliant	不符合 Non-compliant	不適用 N/A	查核事實紀錄 (請具體載明佐證文件) Record of audit findings (please specify supporting documents)
1	配置管理之人員及相當資源 Allocation of management personnel and adequate resources	1-1	是否配置專責人員或組織？ Is a dedicated person or unit assigned?				1.個人資料管理組織相關文件。Documents on the personal data management organization.2.個人資料管理專人名冊。Roster of dedicated personal data managers.
		1-2	是否配置適當資源？ Are adequate resources allocated?				1.相關會議結論或決議事項。Related meeting conclusions or resolutions.2.預算表或資源規劃相關文件。Budget tables or resource-planning documents.
2	界定個人資料之範圍 Defining the scope of personal data	2-1	是否進行個人資料檔案盤點？ Is a personal data file inventory conducted?				盤點清冊或紀錄。 Inventory list or records.
		2-2	是否建立個人資料檔案清冊？ Is a personal data file inventory list established?				盤點清冊或紀錄。 Inventory list or records.
		2-3	是否確實個人資料檔案識別？ Are personal data files properly identified?				盤點清冊或紀錄。 Inventory list or records.
3	個人資料之風險評估及管理機制 Risk assessment and management mechanisms for personal data	3-1	是否進行個人資料檔案風險評估？ Is a risk assessment of personal data files conducted?				1.風險評鑑表。Risk assessment form.2.風險評鑑結果報告。Risk assessment result report.
		3-2	是否針對個人資料檔案風險進行處理？ Are risks to personal data files addressed?				風險處理計畫。 Risk treatment plan.
4	事故之預防、通報及應變 Incident prevention, notification, and response	4-1	是否具備事故通報及應變程序？ Are incident notification and response procedures in place?				內外部通報應變程序，相關人員權責分配等。 Internal/external notification and response procedures, allocation of responsibilities, etc.

項次 No.	查核項目 Audit item	符合 Compliant	不符合 Non-compliant	不適用 N/A	查核事實紀錄（請具體載明佐證文件） Record of audit findings (please specify supporting documents)
	4-2 是否事故發生後採取應變措施？ Are response measures taken after an incident occurs?				事件通報與處理相關紀錄。 Records of incident notification and handling.
	4-3 是否事故發生後於期限內通知當事人？ Are the data subjects notified within the time limit after an incident?				事件通報與通知當事人相關紀錄。 Records of incident notification and notice to data subjects.
	4-4 是否事故發生後採取預防措施？ Are preventive measures taken after an incident?				個人資料事故檢討相關紀錄。 Records of personal data incident review.
	4-5 是否將事故處理情形及補救措施通知本校？ Are the incident handling and remedial measures reported to the University?				通知本校之相關公文或紀錄。 Official documents or records of notification to the University.
5	個人資料蒐集、處理與利用之內部管理程序 Internal management procedures for the collection, processing, and use of personal data	5-1 個人資料蒐集、處理與利用是否具備特定目的並具有法定要件，或依規定取得當事人同意？ Do the collection, processing, and use of personal data have a specific purpose and statutory grounds, or is the data subject's consent obtained as required?			1.特定目的說明。 Statement of specific purpose.2.對應之法定要件說明。Statement of corresponding statutory grounds.3.當事人同意書。 Data subject consent form.
		5-2 特定目的外之利用行為是否符合法定要件？ Does any use beyond the specific purpose meet the statutory grounds?			具特定目的外利用之說明文件。 Documentation for use beyond the specific purpose.
		5-3 是否履行告知義務（未履行告知義務為符合免告知之情形）？ Is the duty to notify fulfilled (non-notification only where an exemption applies)?			履行告知義務之相關紀錄。 Records of fulfilling the duty to notify.
		5-4 是否對複委託方依個資法進行監督？ Is the subcontractor supervised in accordance with the Act?			1.與複委託方間之契約包括個人資料保護相關監督條文、其他監督及管理程序。The contract with the subcontractor includes personal data protection supervision clauses and other supervision and management procedures.2.對複委託方之個人資料保護監督紀錄。 Records of personal data protection supervision of the subcontractor.
		5-5 是否提供當事人權利行使管道？ Are channels provided for data subjects to exercise their rights?			提供當事人權利行使相關管道。 Channels provided for data subjects to exercise their rights.
		5-6 是否將當事人權利行使回覆情形做成紀錄供機關備查？ Are responses to data subjects' exercise of rights			回覆當事人權利行使請求之紀錄。 Records of responses to data subjects' requests to exercise rights.

項次 No.		查核項目 Audit item	符合 Compliant	不符合 Non-compliant	不適用 N/A	查核事實紀錄（請具體載明佐證文件） Record of audit findings (please specify supporting documents)
		recorded for the authority's reference?				
		5-7 契約終止或解除時，是否刪除、銷毀所持有之個人資料？ Upon termination or rescission of the contract, is the personal data held deleted or destroyed?				1.契約或協議等有關個人資料刪除與銷毀之規定。Provisions on deletion and destruction of personal data in the contract or agreement.2.若為延續專案，前期契約或協議等結束時之個人資料刪除及銷毀紀錄。For a continued project, records of personal data deletion and destruction at the end of the prior contract or 3.若為新案，預定執行之個人資料刪除及銷毀之相關程序。For a new project, the planned procedures for deletion and destruction of personal data.
		5-8 契約終止或解除，是否返還個人資料之載體？ Upon termination or rescission of the contract, is the media of personal data returned?				1.契約或協議等有關個人資料刪除與銷毀之規定。Provisions on deletion and destruction of personal data in the contract or agreement.2.若為延續專案，前期契約或協議等結束時之個人資料刪除及銷毀紀錄。For a continued project, records of personal data deletion and destruction at the end of the prior contract or 3.若為新案，預定執行之個人資料刪除及銷毀之相關程序。For a new project, the planned procedures for deletion and destruction of personal data.
		5-9 是否已簽署個人資料刪除、銷毀及載體返還切結書？ Has an undertaking on deletion, destruction, and return of personal data media been signed?				簽署個人資料刪除、銷毀及載體返還切結書之規定及紀錄。 Rules and records regarding signing the undertaking on deletion, destruction, and return of personal data media.
6	資料安全管理及人員管理 Data security management and personnel management	6-1 是否針對個人資料進行去識別化？ Is personal data de-identified?				個人資料去識別化之相關紀錄。 Records of personal data de-identification.
		6-2 是否區分個人資料存取個人帳號及權限？ Are individual accounts and access privileges for personal data differentiated?				個人資料之應用系統帳號及權限設定。 Account and privilege settings of the personal data application system.
		6-3 個人資料是否存放於儲存媒體有加密機制？ Is personal data stored on media with an encryption mechanism?				個人資料檔案之儲存媒體加密機制。 Encryption mechanism for the storage media of personal data files.
		6-4 是否針對個人資料之傳送進行管控？ Is the transmission of				傳輸管理程序或相關規定及紀錄。 Transmission management

項次 No.			查核項目 Audit item	符合 Compliant	不符合 Non-compliant	不適用 N/A	查核事實紀錄（請具體載明佐證文件） Record of audit findings (please specify supporting documents)
			personal data controlled?				procedures or related rules and records.
		6-5	處理個人資料人員是否均簽署保密協定？ Have all personnel handling personal data signed a confidentiality agreement?				簽署保密協定相關紀錄。 Records of signed confidentiality agreements.
		6-6	是否針對個人資料儲存場所施行人員進出管控？ Is entry/exit control implemented for personal data storage locations?				門禁等場所管制進出管理方式及相關紀錄。 Access-control and entry/exit management methods and related records.
7	認知宣導及教育訓練 Awareness promotion and education/training	7-1	處理個人資料之人員是否均接受個人資料保護認知宣導之教育訓練？ Have all personnel handling personal data received awareness education/training on personal data protection?				人員教育訓練或宣導紀錄。 Records of personnel education/training or promotion.
		7-2	是否針對教育訓練課程進行課後評量？ Is a post-course assessment conducted for the training?				課後評量結果紀錄。 Records of post-course assessment results.
8	設備安全管理 Equipment security management	8-1	是否針對處理個人資料設備及環境進行控管之保護？ Are the equipment and environment for handling personal data controlled and protected?				個人資料於攜帶式儲存媒體（如隨身碟）或筆記型電腦之管理方式及安全相關規定。 Management methods and security rules for personal data on portable storage media (e.g., USB drives) or laptops.
		8-2	處理個人資料設備是否安裝防毒軟體並更新？ Is antivirus software installed and updated on equipment handling personal data?				防毒軟體名稱 Antivirus software name： 病毒碼更新日期 Virus definition update date：
		8-3	處理個人資料設備是否設定螢幕保護程式？ Is a screen saver set on equipment handling personal data?				螢幕保護程式設定情形。 Screen saver configuration status.
9	資料安全稽核機制 Data security audit mechanism	9-1	是否定期實施個人資料安全自我評核？ Is a periodic personal data security self-assessment conducted?				提供個人資料安全自我評核紀錄。 Provide records of personal data security self-assessment.
		9-2	是否製作個人資料安全評核報告？ Is a personal data security assessment report produced?				提供個人資料安全評核報告。 Provide the personal data security assessment report.
10	使用紀錄、軌跡資料及證據保存 Retention of usage records, trace data, and evidence	10-1	是否保存因應事故發生所採取行為之紀錄？ Are records of actions taken in response to incidents retained?				事故通報及應變相關表單與紀錄。 Forms and records related to incident notification and response.
		10-2	是否保存提供當事人行使權利之紀錄？ Are records of enabling data subjects to exercise their rights retained?				當事人行使權利相關表單與紀錄。 Forms and records related to data subjects exercising their rights.
		10-3	是否保存個人資料保護教				教育訓練之簽到表或相關

項次 No.			查核項目 Audit item	符合 Compliant	不符合 Non-compliant	不適用 N/A	查核事實紀錄（請具體載明佐證文件） Record of audit findings (please specify supporting documents)
			育訓練紀錄？ Are personal data protection education/training records retained?				紀錄。 Sign-in sheets or related records of the training.
		10-4	是否保存個人資料系統存取紀錄？ Are access records of the personal data system retained?				系統存取 log、權限新增、變動及刪除等紀錄。 System access logs and records of privilege additions, changes, and deletions.
		10-5	是否保存個人資料更正與刪除之紀錄？ Are records of correction and deletion of personal data retained?				個人資料更正、刪除之相關紀錄。 Records related to correction and deletion of personal data.
11	個人資料安全維護之整體持續改善 Overall Continuous Improvement of Personal Data Security	11-1	是否配合法規、技術更新改變，定期檢討個人資料保護措施？ Are personal data protection measures periodically reviewed in line with legal and technological changes?				相關討論會議紀錄。 Records of related discussion meetings.
		11-2	是否針對個人資料安全自我評核結果進行改善？ Are improvements made based on the personal data security self-assessment results?				個人資料安全自我評核結果及改善紀錄。 Personal data security self-assessment results and improvement records.
		11-3	是否依委託機關所提出之建議進行改善？ Are improvements made according to the recommendations of the commissioning authority?				委託機關提出之改善意見及相關改善紀錄。 Improvement recommendations from the commissioning authority and related improvement records.
自評單位填寫人員 Person completing the self-assessment unit				自評單位主管 Head of the self-assessment unit	查核單位 Auditing unit		