**附錄3：業者個人資料蒐集、處理及利用之委外業務監督管理自評表範例**

業者委託資服業者進行個人資料蒐集、處理及利用之業務時，應依「個人資料保護法施行細則」第8條、「數位經濟相關產業個人資料檔案安全維護管理辦法」第19條第1項負監督委外廠商義務。

數位發展部數位產業署提供以下範本，使業者監督委外廠商時，提供給受委託之資服業者自評時參考。

受託廠商名稱： 　　　　(委外廠商資服業者填寫)

自評人員：

自評日期：　　年　　月　　 日

|  |  |  |  |
| --- | --- | --- | --- |
| **項次** | **自評內容** | **自評結果** | **說明** |
| **個資保護政策與安全維護計畫** | | | |
| **1** | 是否訂定個人資料保護管理政策，並對內公開周知？ | □符合  □不符合  □不適用 |  |
| **2** | 是否訂定個人資料檔案安全維護計畫或適當安全維護措施或建置通過第三方驗證之資訊安全管理系統並公布施行？ | □符合  □不符合  □不適用 |  |
| **個人資料生命週期行為規範** | | | |
| **3** | 對於個人資料之蒐集、處理或利用之範圍、類別、特定目的與期間是否明確律定？ | □符合  □不符合  □不適用 |  |
| **4** | 對於個人資料之蒐集、處理、利用、傳輸或刪除，是否訂定管理作業程序並公布施行？ | □符合  □不符合  □不適用 |  |
| **個人資料盤點與風險管理** | | | |
| **5** | 對所保有之個人資料，是否定期實施個人資料盤點作業？ | □符合  □不符合  □不適用 |  |
| **6** | 是否適時維護或更新個人資料檔案清冊？ | □符合  □不符合  □不適用 |  |
| **7** | 是否定期實施個人資料風險評鑑作業？ | □符合  □不符合  □不適用 |  |
| **8** | 對於個人資料風險評鑑結果，是否考量業務性質、個人資料存取環境、個人資料傳輸之工具與方法及個人資料之種類、數量等因素，採取適當之人員、作業、設備及技術之安全管理措施？ | □符合  □不符合  □不適用 |  |
| **人員管理** | | | |
| **9** | 是否訂定人員管理作業程序並公布施行？ | □符合  □不符合  □不適用 |  |
| **10** | 是否定期對內部人員實施資安認知宣導及教育訓練？ | □符合  □不符合  □不適用 |  |
| **11** | 執行個人資料蒐集、處理及利用之人員，是否取得資通安全專業證照？ | □符合  □不符合  □不適用 |  |
| **日常維運作業** | | | |
| **12** | 是否定期識別、審視防火牆、主機系統、資料庫等重要設備之異常告警機制並留存至少5年之LOG？ | □符合  □不符合  □不適用 |  |
| **13** | 系統異動或登入是否取得授權？ | □符合  □不符合  □不適用 |  |
| **14** | 是否進行系統運作與維護之需求評估，並依此建立適當的系統安全檢測機制？ | □符合  □不符合  □不適用 |  |
| **15** | 是否依據各項變更之需求進行變更作業程序，並留存相關紀錄? | □符合  □不符合  □不適用 |  |
| **16** | 是否依據系統各項目標與需求，研擬適當的防護措施檢核表? | □符合  □不符合  □不適用 |  |
| **17** | 是否要求委外廠商定期提出系統安全之風險評估報告? | □符合  □不符合  □不適用 |  |
| **內部稽核** | | | |
| **18** | 是否定期實施資訊安全或個人資料保護之內部稽核並提出稽核報告？ | □符合  □不符合  □不適用 |  |
| **19** | 稽核結果若有不符合法令或有違法之虞或缺失者，是否規劃採取包含修正個人資料保護管理政策及個人資料檔案安全維護計畫之改善及預防措施？ | □符合  □不符合  □不適用 |  |
| **資安事故通報與應變** | | | |
| **20** | 是否訂定資安事故之通報及應變程序，包含知悉資安/個資事故發生或有發生之虞之相關通報時效規定、通報方式、事故調查、處理及改善流程並公布施行？ | □符合  □不符合  □不適用 |  |
| **21** | 是否訂定違反個人資料保護法、其他個人資料保護法律或其法規命令時之通知之事項及採行之補救措施作業程序並公布施行？ | □符合  □不符合  □不適用 |  |
| **受託業務之複委託選任與監督** | | | |
| **22** | 受託業務之複委託事項，是否經委託機關之書面同意後實施？ | □符合  □不符合  □不適用 |  |
| **23** | 是否訂定委託之標準及評估機制並公布施行？ | □符合  □不符合  □不適用 |  |
| **24** | 是否於委託契約或相關文件中明確約定適當之個人資料保護有關事項之監督方式，並留存監督之紀錄？ | □符合  □不符合  □不適用 |  |
| **委託關係終止或解除** | | | |
| **25** | 是否訂定委託關係終止或解除時，個人資料載體之返還，及履行委託契約以儲存方式而持有之個人資料之刪除作業程序並公布施行？ | □符合  □不符合  □不適用 |  |
| **文件化** | | | |
| **26** | 是否對於個人資料之蒐集、處理、利用、國際傳輸或刪除均留存使用紀錄或軌跡資料？ | □符合  □不符合  □不適用 |  |