個人資料風險評估表（範本）使用說明

- 執行個資風險評估時，主要分成「個資重要性」及「發生事故可能性」二大要項，其中將每一細項以三級程度進行評價，並分別賦予不同分數，例如「高」5 分、「中」3 分、「低」1 分，以此來判斷不同風險程度。
  以下說明僅為零售業常見型態，公司或組織仍可依據實際情況進行調整。

一、個資重要性評估

1.個資類別評價

- 評估個資內容的敏感程度，依據個資類別的性質進行評估，通常可區分為特種個資、財務類個資、一般類個資。
  (1)高風險（5 分）：包含有特種個資，病歷、醫療、基因、性生活、健康檢查及犯罪前科。
  (2)中風險（3 分）：包含有財務類個資，例如銀號帳戶、信用卡卡號、薪資、保險等，或包含有重要身分辨識個資，例如身分證字號、護照號碼等。
  (3)低風險（1 分）：僅有一般類個資，例如姓名、生日、聯絡資訊等。

2.當事人影響評價

- 評估發生個資事故會對當事人造成之影響，通常可將當事人區分為客戶（消費者、會員或交易對象）、員工與外部廠商。以零售業而言，若客戶個資外洩可能會被用於詐騙導致財產損失，因此造成之影響較為嚴重屬於高風險。
  (1)高風險（5 分）：客戶。
  (2)中風險（3 分）：員工。
  (3)低風險（1 分）：外部廠商。

3.公司影響評價

- 評估發生個資事故會對公司或組織造成之影響，通常會考量訴訟、賠償、商譽等因素。
  (1)高風險（5 分）：可能會使公司面臨訴訟、可能會使公司付出高額賠償等。
  (2)中風險（3 分）：可能會使公司被媒體報導而影響商譽等。
  (3)低風險（1 分）：可能會使公司付出小額賠償等。

4.重要性總評價

- 重要性總評價是個資重要評估的結果（分數），將「個資類別評價」的分數、

「當事人影像評價」分數及「公司影響評價」的分數加總，即可得出重要性總評價分數。

二、個資侵害發生可能性評估

1.安全措施評估

- 檢視該項個資檔案本身或作業流程是否有採取安全維護措施，及確認安全措施是否符合程序規範。
  (1)高風險（5 分）：未採取任何安全措施，或採取無效之措施。
  (2)中風險（3 分）：已採取安全措施但未符合規範。
  (3)低風險（1 分）：已採取安全措施且符合規範。

2.稽核結果評估

- 檢視於稽核（內稽、外稽皆可參考）發現之缺失或建議改善事項，是否已有進行修正或改善。
  (1)高風險（5 分）：未依稽核結果修正缺失。
  (2)中風險（3 分）：未依稽核結果改善建議事項。
  (3)低風險（1 分）：已改正缺失，或已改善建議事項。

3.委外評估

- 檢視該項個資檔案或作業流程是否有委外蒐集、處理或利用，如果有委外者是否有對委託對象進行監督並評估監督查核結果。
  (1)高風險（5 分）：未對委託對象進行監督，或監督查核結果有重大缺失。
  (2)中風險（3 分）：已對委託對象進行監督且監督查核結果有輕微缺失。
  (3)低風險（1 分）：已對委託對象進行監督且監督查核結果無缺失。

4.曾發生事故

- 檢視該項個資檔案或作業流程是否有發生過個資事故，如果有曾發生過事故則應確認是否有找出事故根因並修正。
  (1)高風險（5 分）：曾發生事故，但未找出或未改善事故根因。
  (2)中風險（3 分）：曾發生事故，但已改善事故根因。
  (3)低風險（1 分）：未發生過事故。

5.侵害發生可能性總評價

- 侵害發生可能性總評價是個資侵害發生可能性評估的結果（分數），將「安

全措施評估」的分數、「稽核結果評估」分數、「委外評估」的分數及「曾發生事故」的分數加總，即可得出侵害發生可能性總評價分數。

三、風險評估總評價

- 風險評估總評價是進行風險評估的最終結果(分數)，將「個資重要性評估」的分數及「個資侵害發生可能性評估」的分數相乘，即可得出風險評估總評價分數。
- 公司或組織應對風險評估總評價**設定高、中、低程度**，例如 210 分以上屬於高風險；110 分至 210 分屬於中風險；110 分以下屬於低風險，對於高風險項目必須要採取因應措施使其風險程度降低，注意中風險項目避免增加風險。