歐盟網路韌性法案簡介

駐歐盟經濟組/2025 年 1 月 13 日

一、前言

近年數位軟硬體產品越來越容易受到成功的網路攻擊，截至 2021 年，全球網路犯罪每年造成的損失達到 5.5 兆歐元，為強化嬰兒監視器、智慧手錶等包含數位零組件之產品之網路安全標準，及要求製造商和零售商確保其產品於完整生命週期之網路安全，歐盟於 2024 年 11 月 20 日公告網路韌性法(Cyber Resilience Act)，以解決歐盟境內許多產品之網路安全水準不足，以及軟硬體缺乏及時安全更新等問題。該法對製造商和零售商導入了強制性網路安全要求，使消費者能更加簡易地識別具有適當網路安全功能之軟硬體產品。

二、法規要點

(一)適用範圍：

1. 依據歐盟網路韌性法(下稱本法)第 2 條規定，本法適用歐盟市場具備數位元素之產品(product with digital element，下稱數位產品)，且該產品之合理可預見用途包含與網路或其他設備進行物理或邏輯資料傳輸，傳輸方式可為直接或間接之方式。

2. 本法不適用歐盟規章 Regulation (EU) 2017/745(醫療設備)、Regulation (EU) 2017/746(體外診斷醫療設備)、 Regulation (EU) 2019/2144(車輛及相關系統元件)、Regulation (EU) 2018/1139(航空器)、Directive 2014/90/EU(船用設備)等所規範之數位產品。

3. 本法不適用數位產品之零組件替換品，亦不適用因國安或國防等目的，設計用來處理機敏資訊之數位產品，本法規定之

義務不應揭露會危及歐盟會員國之國安、公共安全等之資訊。

(二)會員國不應阻礙之事項：本法第 4 條規定，歐盟會員國不應阻礙符合本法規定之數位產品於歐盟境內販售，另針對不符本法規定之數位產品及軟體，在明確標示該數位產品/軟體不符本法規之前提下，歐盟會員國不應阻礙數位產品於商展類似活動進行展示、不應阻礙軟體可於市場上於期限內進行公開測試。

(三)數位產品之要求：本法第 6 條規定，數位產品符合本法附件 1 第 1 部分所列舉之基本網路安全要求(如識別及記錄安全漏洞、防止未經授權之資料存取、永久刪除資料機制等)，且其製造商符合本法附件 1 第 2 部分所規定之網安要求，可在正確安裝及適時更新安全性等前提下，於歐盟市場上販售。

(四)重要之數位產品：本法第 7 條規定，符合本法附件 3 所列舉之數位產品，如身分管理系統、密碼管理器、公鑰基礎設施、實體或虛擬網路介面等，歸類為重要之數位產品，其製造商應遵循本法第 32 條所規定之符合性評鑑程序，確認該產品與製造流程符合本法附件 1 所列舉之網安要求。

(五)關鍵之數位產品：本法第 8 條規定，執委會有權援引授權法案，依據本法附件 4 所列舉產品(如包含保險箱(Security Boxes)之硬體設備、包含安全元件之智慧卡等)之核心功能，判定哪些數位產品將歸類為關鍵之數位產品，該等產品需取得歐盟法規 Regulation (EU) 2019/881 採認之歐洲網路安全認證(至少需取得該認證之「實質」(substantial)保證級別)，以確保該等產品與製造流程符合本法附件 1 所列舉之基本網路安全要求。

(六)高風險 AI 系統：本法第 12 條規定，數位產品倘符合歐盟 AI 法案(Regulation (EU) 2024/1689)第 6 條定義之高風險 AI 系統，需符合歐盟 AI 法案第 15 條有關網路安全之要求，前述網安要求包括符合本法附件 1 所規定之基本網路安全要求，並適用歐

盟 AI 法案第 43 條有關符合性評鑑之規定。

(七)製造商義務：

1. 依據本法第 13、22、28、31 條規定，製造商將本法適用之數位產品於歐盟市場銷售時，須確保其產品之設計、開發和生產符合本法附件 1 第 1 部分所規定之基本網路安全要求，並進行相關網安風險評估，前述風險評估資訊應納入依本法第 31 條規定所應撰擬之技術文件中，該技術文件連同依本法第 28 條規定撰擬之符合性聲明，一併提交至市場監督機構保存至少 10 年。

2. 製造商在整合來自第三方之零組件時應進行盡職調查，確保不致損害數位產品之網路安全；另製造商應確保在支援期(support period)內於識別出零組件之網安漏洞後，應依據本法附件 1 第 2 部分所規定之漏洞處理要求進行修復，前述支援期應至少維持 5 年。

3. 依據本法第 14 條規定，製造商倘發現其數位產品之安全漏洞，應透過依據本法第 16 條由歐盟網路安全機構(ENISA)建立之單一報告平台，同時通知被指定為協調員(coordinator)的電腦安全事件回應團隊 (CSIRT) 及 ENISA。

(八)進口商義務：依據本法第 19 條規定：

1. 進口商應僅將具有符合本法附件 1 第 1 部分規定之基本網路安全要求之數位產品，且該產品之製造商符合附件 1 第二部分規定列舉之基本網路安全要求下，將前述數位產品於歐盟市場販售。

2. 在進口數位產品前，進口商應確保該產品製造商已撰擬技術文件與完成本法第 32 條所述的符合性評鑑程序（如果適用），產品已依據本法第 29-30 條規定貼有 CE 標誌，並附有第 13 條第 20 款規定之歐盟符合性聲明以及附件 2 規定之產品資訊，

該歐盟符合性聲明應於產品於市場銷售後至少 10 年或支持期內（以較長者為準），保留副本供市場監督機構使用。

3. 進口商倘認為其銷售之數位產品不符合本法規定，應立即採取必要糾正措施，以確保數位產品符合本法規定，或撤銷、召回產品（如果適用）。

4. 進口商倘發現其數位產品之安全漏洞，應立即通知產品製造商，倘發現數位產品存在重大網路安全風險，應立即通知產品銷售市場之會員國市場監督機構；

5. 進口商應根據市場監督機構要求，提供所有必要資訊和文件，以證明其進口之數位產品符合附件 1 規定的基本網路安全要求。

6. 倘進口商以其名稱或商標將數位產品於市場販售，或對已於市場銷售之數位品進行重大修改，該進口商應被視為該數位產品之製造商，須遵守本法第 13、14 條之相關規定。

(九)經銷商義務：依據本法第 20、21 條規定：

1. 將數位產品於市場販售前，經銷商應先驗證產品已依據本法第 29-30 條規定貼有 CE 標誌，產品製造商與進口商已遵守本法第 13 條第 15、16、18、19 款及第 19 條第 4 款之相關義務。

2. 經銷商倘根據其掌握之資訊認為數位產品或產品製造商不符合附件 1 規定之基本網路安全要求，在該產品或製造商符合本法規前，經銷商不得將該數位產品於市場販售；另倘數位產品構成重大網路安全風險，經銷商應立即向製造商和市場監管機構通報。

3. 經銷商倘認為其銷售之數位產品不符合本法規定，應立即採取必要糾正措施，以確保數位產品符合本法規定，或撤銷、召回產品（如果適用）。

4. 經銷商倘發現其數位產品之安全漏洞，應立即通知產品製造商，倘發現數位產品存在重大網路安全風險，應立即通知產品銷售市場之會員國市場監督機構。

5. 倘經銷商以其名稱或商標將數位產品於市場販售，或對已於市場銷售之數位品進行重大修改，該經銷商應被視為該數位產品之製造商，須遵守本法第 13、14 條之相關規定。

(十)CE 標誌：依據本法第 29-30 條規定，加貼 CE 標誌應遵守歐盟規章 Regulation (EC) No 765/2008 第 30 條規定之一般原則，包括 CE 標誌僅能由產品製造商或其授權代表加貼、製造商透過加貼 CE 標誌表示該產品符合 CE 標誌之適用要求等；另 CE 標誌應以明顯、清晰、不可磨滅之方式加貼於數位產品上，倘該數位產品為軟體，則 CE 標誌應貼在本法第 28 條所述之歐盟符合性聲明上或軟體產品隨附之網站上。

(十一) 對包括新創公司在內的中小微型企業的支持措施：

1. 依據本法第 33 條規定，會員國應針對微型企業和小企業的需求，適度採取以下行動：

(1). 規劃有關本法之宣傳和培訓活動；

(2). 建立與微型企業和小企業之溝通管道，俾利政府單位就本法之實施提供建議並回答詢問；

(3). 在歐洲網路安全競爭中心(European Cybersecurity Competence Center)的協助下，提供測試和符合性評鑑之相關協助。

2. 會員國可建立網路韌性監管沙盒，為數位創新產品提供受控測試環境，以促進其開發、設計、驗證和測試，以便於市場銷售前確保產品符合本法相關規定。

三、法案實施時間表：依據法規第 71 規定，目前法案已於 2024 年

12 月 10 日生效，並將於 2027 年 12 月 11 日起適用於歐盟全體會員國，其中，第 14 條有關製造商通知義務相關規定，將另於 2026 年 9 月 11 日適用；第 35 條至第 51 條有關會員國向歐盟執委會之通知義務、通知機構(notified body)、會員國間有關執行通知之經驗交流等相關規定，將另於 2026 年 6 月 11 日開始適用。