歐盟資料保護一般規則(General Data Protection Regulation，GDPR)與我國個人資料保護法之重點比較分析

歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過歐盟規則第 2016/679 號「歐盟資料保護一般規則(General Data Protection Regulation，GDPR)」，將自 2018 年 5 月 25 日開始施行，取代 1995 年制定之「資料保護指令 (Data Protection Directive)」，藉以提升及確保對於歐盟境內資料當事人權利保護之一致性(特別是網路活動)，並排除個人資料在歐盟境內流通之障礙。

GDPR 之架構及主要內容與我國個人資料保護法(下稱個資法)之重點比較分析如下：

一、規範對象與適用地域範圍

（一）GDPR：

第 3 條規範境外資料管理者及處理者對於歐盟境內資料當事人基於提供商品、服務或對於資料當事人在歐盟境內之行為監控所為之資料處理活動者，仍有該法之適用。惟有關域外適用效力之規定如何執行，仍待觀察。

（二）我國個資法：

第 51 條規範我國之公務機關及非公務機關於境外對於我國人民個人資料之蒐集、處理及利用，亦適用我國個資法。

二、保護客體-個人資料之定義

（一）GDPR：

第 4 條規範有關識別或可得識別自然人之任何資訊，並明文涵蓋網路識別碼。

（二）我國個資法：

第 2 條規範得以直接或間接方式識別該個人之資料，因此亦涵蓋網路識別碼。

三、資料處理之要件

（一）GDPR：

第 9 條規範禁止處理與民族或種族來源、政治見解、宗教或世界觀確信或所屬工會相關之個人資料，以及得明確識別特定人之基因資料、生物特徵資料，以及個人之健康資料或性生活或性傾向資料，惟基於公共利益等例外情形時允許處理。

（二）我國個資法：

第 6 條明定病歷、醫療、基因、性生活、健康檢查及犯罪前科等 6 種特種個人資料，原則不得蒐集、處理或利用，僅於法定例外情形(如公務機關執行法定職務或協助公務機關執行法定職務等)方得為之。

四、當事人權利

（一）資料刪除權(被遺忘權)

1. GDPR：

第 17 條規範個人資料當事人有特定情事者，得請求資料管理者及處理者刪除連結。

2. 我國個資法：

第 3 條及第 11 條賦予個人資料當事人於蒐集之特定目的消失或期限屆滿時，得請求資料保有者刪除其個人資料的權利。

（二）以可共同操作之格式提供資料(資料可攜權)

GDPR 第 20 條規範資料當事人於特定情形，有權要求以結構的、通常使用的、機器可讀的形式，接收其提供予管理者之資料，並有權將之傳輸給其他管理者。依此，未來網際網路資料服務業者應提供使用者可將所儲存之個人資料以通用格式存取，並提供給

其他業者之服務。此一概念立意良善，惟如何操作仍待相關子法補充規範。而我國個資法並無相關規範。

五、資料管理者之義務

（一）GDPR：

1. 資料保護評估(DPIA)：

第 35 條規範於特別使用新科技之處理方式，且考量該處理之本質、範圍、使用情形及目的後，認為該處理可能導致自然人之權利及自由的高度風險時，控管者應於處理前，實行該處理對於個人資料保護之影響評估。

2. 資料保護長(DPO)：

第 37 條規範有下列情形之一者，管理者及處理者應指定資料保護長：

a、除法院行使其司法權外，公務機關或機構。

b、管理者或處理者之核心活動，包括依其本質、範圍及/或其目的，需要定期且系統性地大規模監控資料主體。

c、管理者或處理者之核心活動，涉及大規模處理特種個人資料。

（二）我國個資法：

第 6 條第 1 項但書第 2 款及第 5 款所稱適當安全維護措施、第 18 條所稱安全維護事項、第 19 條第 1 項第 2 款及第 27 條第 1 項所稱適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施。而上開措施，依個資法施行細則第 12 條第 2 項規定，得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例

為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善。上開個資法及其施行細則規定，已就公務機關及非公務機關得採取之安全維護措施之程序及內容為例示規範，而各中央目的事業主管機關並可將上開安全維護措施項目列為例行性業務檢查之項目。

六、主管及監督機關

（一）GDPR：

第 51 條規範各會員國除法院及司法權外應設立至少一個獨立公務機關，監督 GDPR 之適用。

（二）我國個資法：

個人資料保護之行政管理採分散式管理，由非公務機關之中央目的事業主管機關執行下列權限，以確保個人資料保護制度之執行:

1. 國際傳輸之例外禁止(個資法第 21 條)。

2. 行政檢查權(個資法第 22 條)。

3. 糾正權(個資法第 25 條)。

4. 指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法，並授權由中央目的事業主管機關訂定辦法(個資法第 27 條第 2 項、第 3 項)。

5. 行政裁罰權(個資法第 47 條至第 50 條)。

七、跨境傳輸

（一）GDPR：

就歐盟境內之個人資料原則禁止跨境傳輸至歐盟以外之地區或國家，須符合下列情形之一者，方得為之：

1.擬傳輸地區經評估具備「適當保護水平」(GDPR 第 45 條）。

2.資料管理者已提供適當保護措施（GDPR 第 46 條)。

(1)訂有具拘束力之企業守則。

(2)採用標準契約條款。

(3)訂有經核准之行為守則。

(4)取得資料保護認證或資料保護標章及標誌。

3.當事人明確同意(GDPR 第 49 條)。

4.履行契約或依當事人要求，為締約前之必要措施(GDPR 第 49 條)。

5.基於重要公共利益之維護(GDPR 第 49 條)。

6.為主張、行使或防禦法律上之請求權所必要(GDPR 第 49 條)。

7.基於保護當事人之重要利益所必要(GDPR 第 49 條)。

8.依法辦理之登記作業，而向公眾提供資訊(GDPR 第 49 條)。

（二）我國個資法

第 21 條就我國個人資料跨境傳輸至境外，雖原則上不禁止，惟非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之，亦得防止我國人之個人資料不當國際傳輸：

1.涉及國家重大利益。

2.國際條約或協定有特別規定。

3.接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

4.以迂迴方法向第三國（地區）傳輸個人資料規避本法。

八、救濟與處罰

（一）GDPR：

第 83 條，違反 GDPR 規範者，最高得處以 2,000 萬歐元或其年度總營收 4%之罰鍰，適用對象限於企業，未針對自然人或公務機關之違反行為制定處罰規範，而係委由各會員國自行訂定有效、適當且具懲戒性的罰則。

（二）我國個資法：

非公務機關違反個資法規定者，中央目的事業主管機關或直轄市、縣（市）政府得按次處新臺幣 2 萬元以上，20 萬元以下；或 5 萬元以上，50 萬元之罰鍰（個資法第 47 條至第 49 條參照）。惟我國個資法第 41 條及第 42 條另定有刑事責任，併予敘明。

綜上，依 GDPR 之規範，其適用對象範圍，除歐盟境內設有分支機構之資料管理者及處理者之外，即便資料管理者或資料處理者於歐盟境內並未設立分支機構，但其在跨境提供商品或服務的過程中，如有蒐集或處理歐盟居民之個人資料者，仍應符合 GDPR 之規範要求，否則將受有鉅額罰鍰。此一適用範圍之擴張，對於我國電子商務產業及經營對外貿易之企業，勢必大幅提升其法規遵循成本，甚至形成貿易障礙。

關於GDPR之規範內容,在當事人之權利部分,除以往之資料查詢、複製、更正及刪除權之外，更進一步賦予當事人得請求資料管理者及

處理者刪除連結(被遺忘權)、要求以可共同操作之格式提供資料(資料可攜權)等權利。在資料管理者部分，新增資料保護影響評估、資料保護長等制度。惟 GDPR 諸多新穎性規範，實務上究應如何運作，仍待歐盟第 29 條資料保護工作小組（Article 29 Data Protection Working Party）持續訂定規範加以補充，我國並應持續密切觀察 GDPR 施行情形以為因應借鑑。