達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

跨境隱私管理趨勢及GDPR域外效力

達文西個資暨高科技法律事務所　所長
葉奇鑫 (奇哥/Simon)

2019/09 於通訊傳播事業個資實務專題講座

- 1995年律師、司法官考試及格
- 美國富蘭克林皮爾斯法學院研究
- 東吳大學法學碩士
- 交通大學電子工程系工學士

現任

- 達文西個資暨高科技法律事務所 所長
- 東吳大學法律研究所 兼任助理教授
- 國發會 個資法諮詢委員
- 智慧財產局 著作權顧問暨調解委員
- 財政部、交通部、勞動部開放資料諮詢委員
- 台灣網際網路暨電子商務協會(TIEA) 監事
- 高科技法務經理人協會(TILO) 理事
- 台灣數位安全聯盟(TWCSA) 理事
- 展翅協會 理事

曾任

- 露天拍賣 營運長
- eBay交易安全長
- 法務部檢察司、資訊處檢察官
- 板橋地檢署電腦犯罪與智慧財產權專組檢察官
- 「霍夫曼計算法」程式設計人
- 刑法第36章妨害電腦使用罪章草擬人

GDPR背景簡介

GDPR是什麼?

General Data Protection Regulation

台灣翻譯為歐盟「通用資料保護規則」，翻譯為「規則」可能引起誤解，只要理解為歐盟個資法即可

取代1995年歐盟個資保護指令(Directive 95/46/EC)

個資保護指令衍生出歐盟各成員國標準不一之個資法，造成企業適用上的困擾

GDPR於2016年公布，2018年5月25日生效，直接適用於歐盟28個會員國，無須各國採行為內國法

為什麼我們必須認識GDPR?

- 天價罰則
- 適用範圍超廣
- 個資定義擴大
- 當事人權利增加
- 新增DPIA、個資長(DPO)、Privacy by Design/Default、Codes of Conduct等企業遵循規範
- 個資外洩事故通知新規定
- 跨境傳輸限制

適足性認定可能影響台灣未來個資法修法方向

自由財經 財經政策 Strategy 國際財經 International 證券產業 Securities 房產資訊 Estate 財經週報 Weeklybiz 基金查詢 Fund

爭取歐盟GDPR適足性認定 國發會：去年底已遞件

讚 LINE

2019-02-18 19:37

GDPR施行後，目前僅日本取得適足性認定，若加計歐盟「95指令（1995年個人資料保護指令）時期，則有13個國家或地區取得歐盟適足性認定，台灣也在去年12月向歐盟遞交自我評估報告。（資料照）

https://ec.ltn.com.tw/article/breakingnews/2702576

研究GDPR之準備動作

下載GDPR中文翻譯

閱讀GDPR條文及Recital

注意WP之意見(含Guideline)

企業(組織)因應GDPR之步驟

一、是否適用GDPR?

二、是否可能將業務適當調整後不適用GDPR?

三、差異性分析(Gap Assessment)

四、修改隱私權條款(告知)及當事人同意

五、符合跨境傳輸之要求

六、強化DPIA、個資長(DPO)、Privacy by Design/Default等企業遵循規範

七、注意個資事故通知規定

從GDPR看世界個資法趨勢

趨勢一 打不贏就加入

一、適足性認證

我國於2018年遞件申請，未來修法方向?

二、美國隱私盾

三、歐盟、日本2018年雙邊承認

四、個資多邊協定架構：APEC CBPR

跨境傳輸之條件之一

安全第三國 Art. 45
歐盟執委會認為該國（地區、國際組織、特定部門）個資保護已達適足性要求(adequate level of protection)
**隱私盾(EU-US Privacy Shield) Art. 45 Sec. 9，2017年4月已有1800家企業、組織加入隱私盾

當事人明示同意 Art. 49 Sec. 1 lits. a

標準個資保護契約條款（Standard Contractual Clauses, SCC） Art. 46 Sec. 2 lits. c,d
需經歐盟執委會或監管機關採行，可以用台灣消保法定型化契約應記載及不得記載事項來理解SCC

拘束力企業守則（Binding Corporate Rules, BCR） Art. 46 Sec. 2 lits. B, Art. 47
適合企業集團，但目前採行僅不到100個集團

跨境傳輸之條件之二

行為守則(Codes of Conduct) Arts. 40, 41

- 須經監管機關審核

認證(Certification) Arts. 42, 43

- ISO? BSI? EuroPrise?

履行契約所必須 Art. 49 Sec. 1 lits. b, c

- 例如旅行業

公共利益 Art. 49 Sec. 4

當事人重大利益 Art. 49 Sec. 1 lit. f

控管者利益大於當事人權利與自由 Art. 49 Sec. 1 subpara.

- 新規定，但有很多限制，例如：不重複、數量有限之當事人、具備適當安全維護措施、通知等等

非歐盟企業（組織）須在歐盟設代表

趨勢二 單一獨立主管機關

◆ 請問：下列何者為通訊傳播業之個資法主管機關?

中華民國 法務部 Ministry Of Justice

國家通訊傳播委員會 NATIONAL COMMUNICATIONS COMMISSION

國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

TAIPEI 臺北市政府 Taipei City Government

個資法之法制主管機關已變更

公告個人資料保護法及個人資料保護法施行細則相關條文涉及原管轄機關為法務部者變更為國家發展委員會

2019-01-15

發文單位：法務部
發文字號：法律 字第 10803500010 號
發文日期：民國 108 年 01 月 10 日
資料來源：行政院公報 第 25 卷 10 期 2763 頁
相關法條：行政程序法 第 11 條（104.12.30）
個人資料保護法 第 53、55 條（104.12.30）
個人資料保護法施行細則 第 33 條（105.03.02）
要　　旨：公告個人資料保護法及個人資料保護法施行細則相關條文涉及原管轄機關為法務部者，變更為國家發展委員會
主　　旨：為配合一百零七年十二月十二日修正發布之法務部處務規程第八條及第十八條修正條文，公告個人資料保護法及個人資料保護法施行細則相關條文涉及原管轄機關為法務部者，變更為國家發展委員會。
依　　據：行政程序法第十一條第二項規定。
公告事項：「個人資料保護法及個人資料保護法施行細則管轄變更法律及法規命令條文表」。

個人資料保護法及個人資料保護法施行細則管轄變更法律及法規命令條文表

序號	法律名稱	條項款目	管轄事項變更情形
1	個人資料保護法	§53、§55	本法各該規定所列屬「法務部」之權責事項，改由「國家發展委員會」管轄。
2	個人資料保護法施行細則	§33	本細則各該規定所列屬「法務部」之權責事項，改由「國家發展委員會」管轄

註：為茲簡明，條項款目欄中，各條、項、款、目等，分以下列方式表達：條→§（條號以阿拉伯數字表達）、項→Ⅰ（羅馬符號）、款→（1）（括弧內置阿拉伯數字）、目→○1（圓圈內置阿拉伯數字），目以下則以「之○（阿拉伯數字）」表達。

趨勢二 單一獨立主管機關

一、台灣個資法主管機關採分散式設計

- 「法制主管機關」
- 中央目的事業主管機關
- 縣市政府

二、何謂「獨立」？

三、港澳個資法主管機關薪水福利知多少？(淺談個資保護專業人員之職場未來)

趨勢三 重罰

一、GDPR最重可罰多少?

二、台灣個資法最重可罰多少?

三、Google今年一月被罰多少?

GDPR天價罰則之一

Max (2000萬歐元，前一會計年度全球4%營業額)　Art. 83 Sec. 5

違反個資處理原則、當事人同意、特種個資處理　Arts. 5,6,7,9

違反當事人權利　Arts. 12 to 22

違反跨境傳輸　Arts 44 to 49

違反開放會員國制定之法律義務　Chapter IX

妨礙主管機關執法　Art. 58 Sec. 1, 2

GDPR天價罰則之二

Max (1000萬歐元，前一會計年度全球2%營業額)　Art. 83 Sec. 4

資料控管者與處理者違反: 兒童同意相關規定(Art. 8); 控管者與處理者義務 (Arts. 25 to 39); 個資保護認證相關規定 (Arts. 42, 43)

認證機關違反　Arts. 42, 43

行為守則(Codes of Conduct)監督機關違反　Arts 41 Sec. 4

不需要個資外洩即可重罰

GDPR最重可罰**2,000萬歐元**或前一會計年度**全球4%營業額**。

GDPR之透明性

Rec. 39
It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.

Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

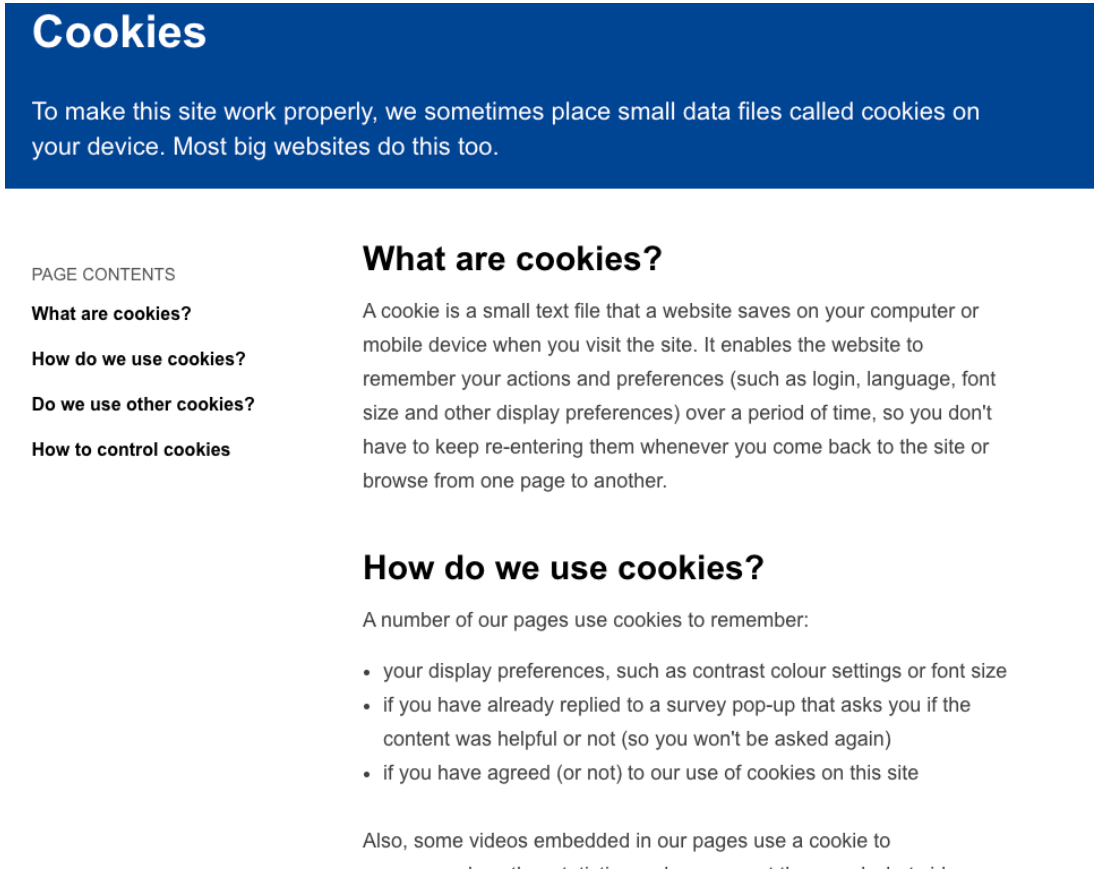
趨勢四 個資定義擴大

「個人資料」係指有關識別或可得識別自然人（「資料當事人」）之任何資訊；可得識別自然人係指得以直接或間接地識別該自然人，特別是參考諸如姓名、身分證統一編號、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素之識別工具。

Art. 4 No. 1
'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

◆ **討論：online identifier是否包含Cookie？IP？(GDPR Recital 30)**

歐盟執委會對蒐集Cookie之告知



趨勢五 域外效力

據點原則 Art. 3 Sec1

本規則適用於在歐盟境內設有據點之控管者或處理者處理個資的業務活動，不論該處理行為是否發生於歐盟境內。

域外效力 Art. 3 Sec2

本規則對於未在歐盟境內設有據點，但處理歐盟境內資料當事人之個資，且該處理個資之業務活動與下列事項有關的控管者或處理者，亦有適用：

(a)對歐盟境內資料當事人提供商品或服務，不論是否向資料當事人收取費用；或

(b)監控資料當事人於歐盟境內之行為。

- **討論：台灣電商網站、銀行、電信公司是否適用GDPR?**

如何判斷是否落入GDPR規範?

Rec. 23

In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.

Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation)

域外效力之示例

指導原則 3/2018

歐盟一般資料保護條例之地域範圍

第 3 條

（公眾諮詢版本）

於 2018 年 11 月 16 日通過

Example 10: A bank in Taiwan has customers that are residing in Taiwan but hold German citizenship. The bank is active only in Taiwan; its activities are not directed at the EU market. The bank's processing of the personal data of its German customers is not subject to the GDPR.

示例 10：一家位於台灣的銀行，其客戶雖居住於台灣，但持有德國國籍。該銀行的活動範圍僅限於台灣而非針對歐盟市場。位於台灣的銀行處理德國客戶的個人資料不受 GDPR 拘束。

Example 11: The Canadian immigration authority processes personal data of EU citizens when entering the Canadian territory for the purpose of examining their visa application. This processing is not subject to the GDPR.

示例 11：加拿大移民署在歐盟公民進入加拿大領土時，處理歐盟公民的個人數據資料，以審查其簽證申請。此處理不受 GDPR 拘束。

(Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation)

趨勢六 個資保護專業化 / 獨立化

誰需要指定個資保護長(DPO, Data Protection Officer)?

- 源於德國之制度，即使歐盟大部分的國家也對DPO很陌生。
- 歐盟理事會、執委會和議會對DPO之意見也不盡相同，例如：歐盟議會認為12個月內蒐集超過5000筆個資，即應強制指派DPO，而執委會認為應以員工數250人為標準。
- 公務機關 (Art. 37 Sec. 1 lit. a & Art. 37 Sec. 3)
  - ✓ 公務機關應指派DPO。
  - ✓ 考量公務機關之組織與規模，多數公務機關可共同指派一位DPO。
- 非公務機關 (Art. 37 Sec. 1 lits. b, c & Art. 37 Sec. 4)
  - ✓ 資料控管者或處理者之核心業務(Core activities)涉及：
    (1) 大規模進行常態性(regular)與系統性(systematic)之個資監控。
    (2) 大規模處理特種個資(Art. 9)和刑案個資(Art. 10)。
  - ✓ 集團事業可為整個集團指派一位DPO。
  - ✓ 歐盟或會員國可要求同業公會指派DPO。

◆ **討論：** 法院是否需要指派DPO?

資料保護長 (DPO)之資格

- 應具備個資保護專業 (Art. 37 Sec. 5)。
  德國實務以法律、技術和組織三方面評估DPO之適任度。
- DPO一定必須由企業雇用嗎？(Art. 37 Sec. 6)
  - ✓ DPO可以是內部雇用，也可以聘請外部專家擔任DPO。
  - ✓ 大企業較適合內部雇用DPO，中小企業較適合聘請外部DPO。
- DPO有任期規定嗎?
  - ✓ GDPR並未就任期做規定，但GDPR草案曾建議任期至少2年，可為參考。
- DPO限於自然人嗎?
  - ✓ GDPR未明文排除法人擔任DPO之資格，但在德國仍有爭議。

資料保護長 (DPO)之獨立性

- 組織應確保...
  - ✓ DPO適當且即時參與個資保護議題 (Art. 38 Sec. 1)
  - ✓ DPO有足夠之資源 (Art. 38 Sec. 2)
  - ✓ DPO不需接受任何關於其執行任務之指示 (Art. 38 Sec. 3)
  - ✓ DPO不因其執行任務而受免職或處罰 (Art. 38 Sec. 3)
  - ✓ DPO應直接向最高管理階層負責 (Art. 38 Sec. 3)
  - ✓ DPO可同時執行其他任務，但不可有利益衝突 (Art. 38 Sec. 6)

- 不適宜被指派為DPO之人：技術長、執行長、財務長、行銷長、業務主管及所有可能決定資料蒐集目的和使用方式之人。

資料保護長 (DPO)之任務

- DPO之任務至少包含 (Art. 39 Sec. 1):
  - ✓ 告知並建議組織及其受雇人關於法律上之資料保護義務
  - ✓ 監督GDPR之法規遵循
  - ✓ 認知提升與教育訓練
  - ✓ 當組織執行DPIA時，提供建議
  - ✓ 擔任監管機關之窗口，並與監管機關合作
  - ✓ 擔任當事人之窗口(Art. 38 Sec. 4)
  - ✓ 保密義務(Art. 38 Sec. 5)

◆ 討論：DPO是否負連帶民事賠償責任?

趨勢七 強調個人資訊自主權

GDPR 6大原則

- 合法性、公平性、透明性 (Lawfulness, fairness, transparency)
- 目的限制原則 (Purpose limitation)
- 資料最小化原則 (Data minimisation)
- 正確性原則 (Accuracy)
- 儲存限制原則 (Storage limitation)
- 完整性與機密性原則 (Integrity and confidentiality)

GDPR 當事人權利

- 近用權(Right to Access)
- 更正權(Right to Rectification)
- 刪除權(Right to Erasure)(延伸出被遺忘權)
- 限制處理權(Right to Restriction of Processing)
- ✖ 資料可攜權(Right to Data Portability)
- 異議權(Right to Object)
- ✖ 自動化決策與剖析(Automated individual decision-making, including profiling)

趨勢七之一 有效同意要件嚴格

- 有效同意之要件

  1. 自由性 (Free/Freely given)
  2. 特定性 (Specific)
  3. 知情性 (Informed)
  4. 非模糊之意思表示 (Unambiguous indication of wishes)

趨勢七之二 資料可攜權

- **Art. 20 Sec. 1**

  資料當事人應有權以有結構、普遍使用且機器可讀之形式，獲得其提供予控管者之資料，並有權將之傳輸給其他控管者，而不受其提供個人資料之控管者之妨礙。

- **Art. 20 Sec. 2**

  如技術許可時，資料當事人應有權使該個人資料由一控管者直接傳輸予其他控管者。

◆ **危機即轉機：Open Banking**

趨勢七之三 剖析與自動決策拒絕權

- **Art. 22 Sec. 1**

  僅基於自動化處理(包括剖析)所做成，而對資料當事人產生法律效果或類似之重大影響之決策，資料當事人應有權不受該等決策拘束。

- **Art. 20 Sec. 2**

  如技術許可時，資料當事人應有權使該個人資料由一控管者直接傳輸予其他控管者。

趨勢八 預防重於治療

趨勢八之一 DPIA (Data Protection Impact Assessment)

- **DPIA是一種針對高風險之預防性個資保護措施**

  在以新興科技處理個資的情況，依該處理個資行為的性質、範圍、內容及目的，將對自然人的權利與自由產生造成高度風險的可能性時，控管者應在處理個資之前，事先對於預定處理個資行為對個人資料的保護執行評估。對於存有類似高度風險的類似處理個資行為得僅執行單一評估。

- Art. 35 Sec. 1

  Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

何時需要做DPIA?

- 有三種情形特別必須做DPIA： (Art. 35 Sec. 1)

  a. 以自動化方式，包含剖析，而系統性及廣泛性對自然人進行評估，且依評估結果對該自然人作出法律上或相似重要影響之決定;

  b. 大規模處理第9條第1項的特種個資，或第10條的刑案個資;

  c. 對公眾場域進行大規模的系統性監控。

- 如有必要，控管者應至少於處理個資行為之風險有所改變時，審查以評估個資處理行為是否遵循個資保護衝擊評估。Art. 35 Sec. 11

- 討論:

  一、企業導入DLP(Data loss prevention)系統前，是否需做DPIA?

  二、個人醫生、律師是否需做DPIA? (REC. 91)

DPIA之內容

- DPIA內容之最低要求： (Art. 35 Sec. 7)
  a. 對預定處理個資之行為及目的作系統性描述，如適用時，包含控管者處理個資的正當利益;
  b. 評估該處理個資行為依其目的之必要性與合比例性;
  c. 評估第1項所稱對資料當事人之權利與自由可能造成的風險;
  d. 預定因應風險的措施，包含依資料當事人或其他相關之人的權利與正當利益所採取確保個人資料之保護及舉證遵循本規則義務的防護措施、安全措施與機制。
- 在有指派個資保護長的情況，控管者在執行個資保護衝擊評估時，應徵詢其建議。Art. 35 Sec. 2
- 討論：DPIA應該由DPO執行嗎?

趨勢八之二 預設隱私設計(Privacy by Design/Default)

- 違反將被處以1000萬歐元或2%全球營收(Art. 83 Sec.4)，但要如何執行？違反到什麼程度才會被處罰？仍屬不確定之法律概念，但可透過認證證明已符合要求(Art. 25 Sec. 3)。
- Privacy by Design(Art. 25 Sec. 1)：控管者在決定如何（或正在）處理資料時，應將技術上或組織上之保護措施，有效的納入處理程序中，以落實資料保護，條文中並以假名化及資料最小原則為舉例。
- Privacy by Default(Art. 25 Sec. 2)：控管者應採取技術上或組織上之措施，預設狀態應僅處理特定目的內必要範圍內之個資（個資數量、處理程度、儲存期間等），並確保不被不特定人使用。此即所謂之隱私友善性設計Privacy Friendly，目的在確保系統預設狀態可提供使用者最大隱私。

謝謝聆聽

THANKS FOR YOUR ATTENTION

達文西個資暨高科技法律事務所

10089 台北市中正區羅斯福路三段162號3樓

Tel：02-2367-0902