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

個資法之修法趨勢初探

達文西個資暨高科技法律事務所　所長
葉奇鑫 (奇哥/Simon)

2020/09/14

歡迎訂閱【達文西個資週報】

- 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 法律系兼任助理教授
- 電腦稽核協會理事長
- 國發會 個資法諮詢委員
- 智慧局著作權 顧問暨調解委員
- 永豐金控 董事
- 台灣網際網路暨電子商務協會 監事
- 高科技法務經理人協會 理事
- 台灣雲端安全聯盟 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

萬物皆個資？

首例！床單有個資 旅館賣抓姦者判賠房客8萬

Yahoo奇摩（綜合報導） | 2.2k 人追蹤 追蹤

2019年5月12日 上午7:05

177 則留言

司法判決首例！國營單位陳姓與胡姓公僕疑偷情，陳妻僱請徵信社抓姦，高市某商旅將兩人用過未清洗的床單賣給徵信業者，法官因認為床單上會留下毛髮和唾液等「個資」，判決商旅和販售的女員工須賠償房客8萬元，業者不滿已提上訴。

最新 焦點 熱門 微視蘋 娛樂時尚 財經地產 愛播網 社會 國際 政治 生活 火線 3C車市

偷情「原汁床組」賣徵信社　旅館挨告逆轉判免賠

出版時間：2019/05/15 21:00

一名胡姓女公務員前年和一名陳姓人夫到高雄橙屋商旅開房間歡度情人節，不料隔天一早遭陳妻會同徵信社人員報警捉姦，事後陳男、胡女不滿當天退房後，旅館將他們用過的床單、被單、毛巾賣給徵信社，提告求償60萬元；一審認為旅館轉賣房客用過的床組，侵害房客資訊隱私權，判旅館與員工連帶賠償8萬元，但二審高雄高分院認為陳男、胡女先侵害陳妻配偶權，事後向旅館求償無理由，加上床單送驗並未驗出兩人DNA，今逆轉改判旅館勝訴免賠。全案確定。對於逆轉勝訴，橙屋商旅不願回應。

嘲諷皆個資？

速食店嗆房東「離兩次婚」 房客違反個資法判4月

房客速食店嗆房東「離兩次婚」，違反個資法判4月。（記者鄭淑婷攝）

2019-11-12 19:01:39

［記者鄭淑婷／桃園報導］桃園市鄭姓房東將房子租給鍾姓房客，卻衍伸出租屋糾紛還為此涉訟，去年4月24日鄭姓房東在丈夫、友人陪同下，與鍾姓房客相約調解仍無共識，結束後3人轉往速食店用餐，豈料，點餐時雙方又巧遇，鍾姓房客不顧用餐人潮，當場對著鄭姓房東及其丈夫指名道姓嗆「妳嫁了兩次都嫁到很爛的老公」、「妳們兩個小學老師怎麼當的，怎麼有資格教學生，欠錢不還」，鄭姓房東及其丈夫不滿婚姻狀態被揭露，氣得到警局提告違反個資法、公然侮辱罪，桃園地院法官審結

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（2020又無效？）

三、歐盟、日本2018年雙邊承認

四、個資多邊協定架構：CBPR

Schrems II Confirms Validity of EU Standard Contractual Clauses, Invalidates EU–U.S. Privacy Shield

JULY 2020 | COMMENTARIES

In Short

The Situation: The Court of Justice of the European Union ("CJEU") has ruled that international data flows under the European Union's comprehensive data protection regime, the GDPR, can continue to be based on EU Standard Contractual Clauses if properly monitored, while the EU–U.S. Privacy Shield has been declared invalid.

https://www.jonesday.com/en/insights/2020/07/schrems-ii-confirms-validity

趨勢二 單一獨立主管機關

◆ 請問：下列何者為銀行之個資法主管機關？

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

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？

https://www.ithome.com.tw/news/139122

趨勢三 重罰

一、請問：GDPR最重可罰多少？

二、請問：台灣個資法最重可罰多少？

三、請問：Google於2019年一月被罰多少？

趨勢三 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**。

趨勢四 一般及特種個資之定義

「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 SEC. 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)

趨勢四 一般及特種個資之定義

揭露種族或人種、政治意見、宗教或哲學信仰或貿易聯盟會員之個人資料、以及基因資料、用以識別自然人之生物特徵識別資料、 與健康相關或與自然人之性生活或性傾向有關個人資料之處理，應予禁止。

Art. 9 SEC. 1
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person‘s sex life or sexual orientation shall be prohibited.

Apple Watch Series 6引進血氧含量監測watchOS 7將升級救命功能?

趨勢五 假名、匿名之釐清

去識別化: 匿名化 vs. 假名化
Anonymisation vs. Pseudonymisation

Rec. 26 GDPR

去識別化之資料不適用GDPR，反之，假名化後仍適用GDPR

「假名化」係指處理個人資料之方式，使該個人資料在不使用 額外資訊時，不再能夠識別出特定之資料主體，且該額外資料 已被分開存放，並以技術及組織措施確保該個人資料無法或無可識別出當事人。

Art. 4(5)

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Rec. 26 GDPR

個人資料保護原則應適用於有關識別或可得識別當事人之任何資訊。已假名化之個人資料，且可透過使用額外資訊而識別出當事人身分者，應被認為屬於可得識別之當事人的資訊。為決定當事人是否可被識別，應考慮到所有可合理使用之方法，例如由控管者自己或透過他人指認以直接或間接地識別該當事人。為確認何為可合理使用作為識別當事人之方法，應考慮所有客觀因素，諸如：識別所需之成本與時間，並考慮到資料處理當時現有之技術及科技發展。因此，資料保護原則不適用於匿名資訊，亦即並非已識別或可識別當事人之資訊，或以使資料主體不可或不再可識別之方式而成為匿名之個人資料。因此，本規則無涉於此類匿名資訊之處理，包括為統計或研究目的所為之者。

資料來源：https://www.jcic.org.tw/main_ch/fileRename/fileRename.aspx?uid=1566&fid=1103&kid=2

趨勢六 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。

趨勢六 域外效力

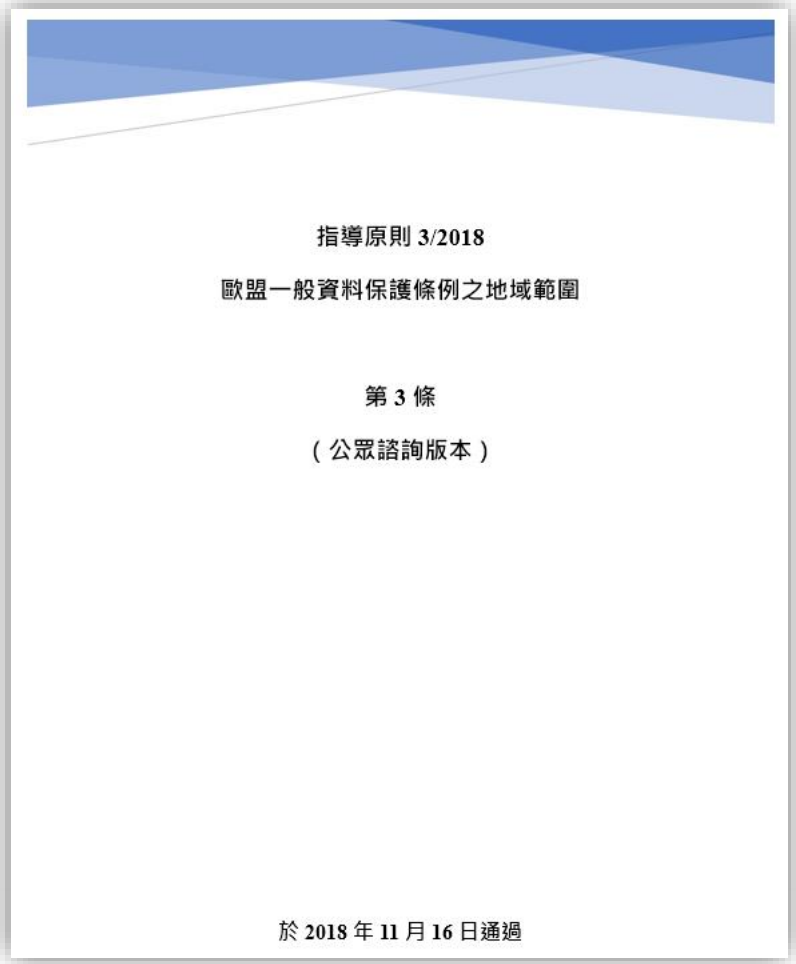
Rec. 23
In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.

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.

◆ **討論：公司如何不落入GDPR規範？**

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

趨勢六 域外效力



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。

趨勢七 世界個資法均GDPR化？

一、公務與非公務機關一視同仁？

二、蒐集、處理、利用是否需要區分？

三、控管者與處理者之區分？

趨勢七 世界個資法均GDPR化？

四、個資事故發生後，應通報主管機關或是當事人？

五、DPIA？DPO？

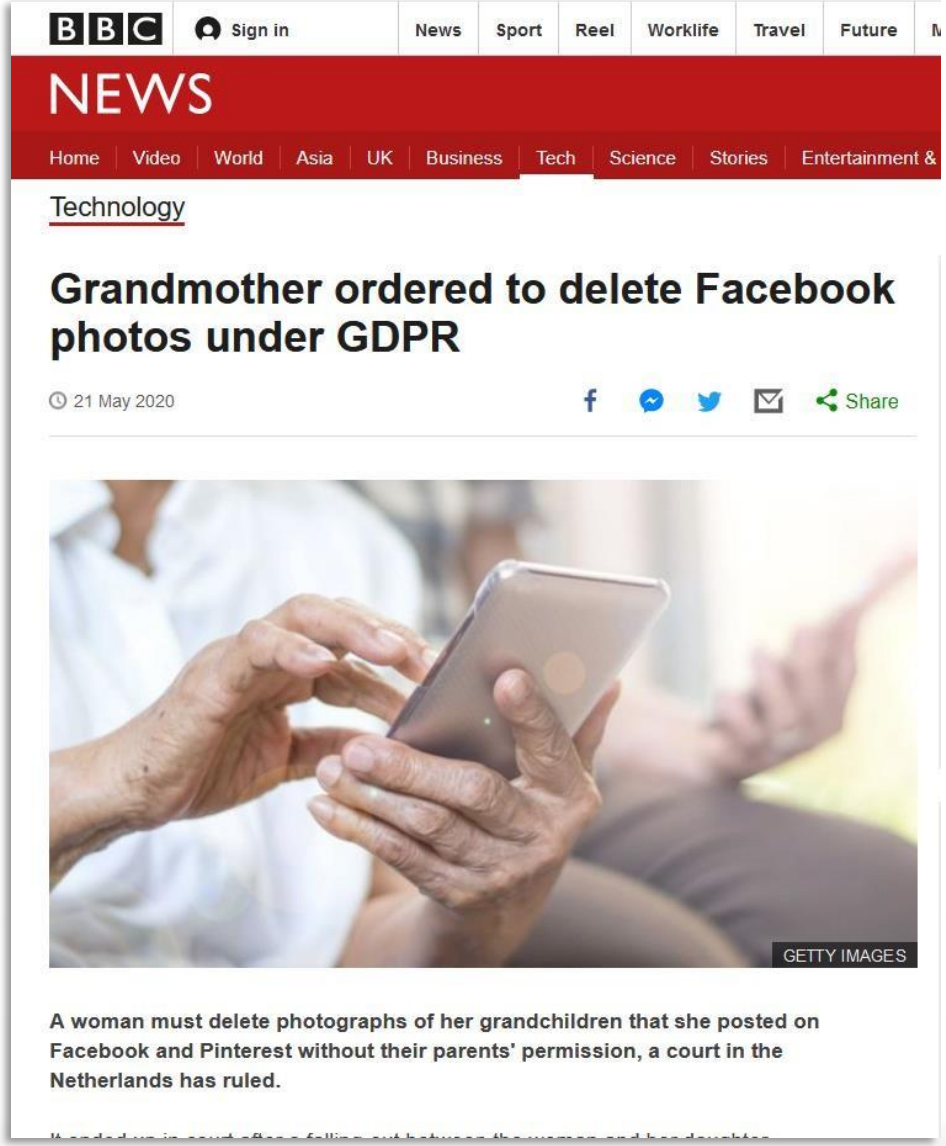
六、個資跨境傳輸原則許可？

趨勢八 強調個人資訊自主權

有效同意之要件：

1. 自主性 (Free/Freely given)
2. 特定性 (Specific)
3. 積極性 (Unambiguous indication of wishes)
4. 能有效撤回同意 (Withdrawal of consent)

個資&隱私保護存在日常生活



2020年5月，荷蘭法院判決認定，在社交網路上po親 友生活照可能適用GDPR、須經當事人同意：

1) 荷蘭一位阿嬤在Facebook與Pinterest上傳三位未成年外 孫的照片，遭到其女兒的反對。女兒經多次溝通無果， 直接向法院提告
2) 法院認為，雖然自然人所為之「單純」（purely）個人 或家庭活動並無GDPR之適用，但這位阿嬤並未對其 Facebook或Pinterest帳號進行保護設定，三位外孫的照 片可能被散布、流入第三方手中，或在Google等搜尋引 擎上搜尋而得。因此，阿嬤的行為非屬「單純」個人或 家庭活動，GDPR適用於該案
3) 法院判定阿嬤之行為未經未成年人之法定代理人同意， 已構成違法，當刪除照片並繳納罰鍰

有效的同意注重品質

自主性

- 不受制於不對等權力
- 不綑綁其他條件
- 不同目的需要分別表達同意
- 拒絕&撤回同意不會受到不利益

有效的同意注重品質

特定性

- 有線電視業者徵求訂戶同意， 依照收視紀錄分析推播個人化推薦節目
- 如日後決定將訂戶收視紀錄提供第三方， 寄送/播送精準廣告，需要另行取得同意

有效的同意注重品質

積極性

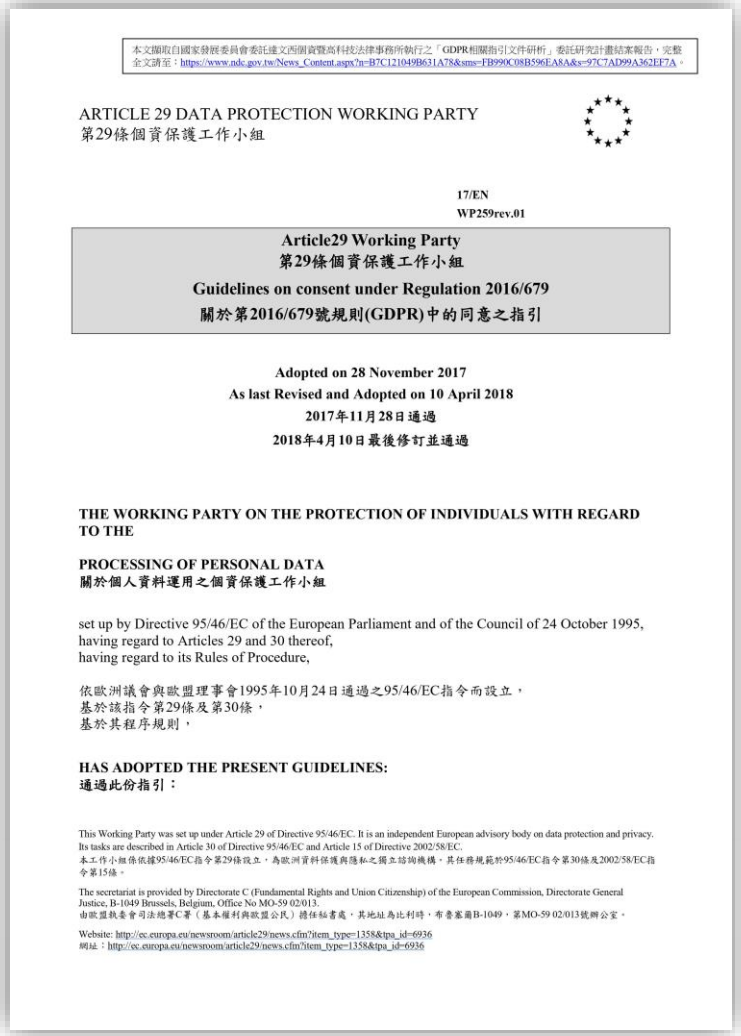
- 預先勾選同意=無效
- 單純沉默、不作為或繼續使用服務，不視為同意

有效的同意注重品質

能有效撤回同意

- 撤回同意方式應和給予同意方式相同簡易
- 以點擊滑鼠、滑動螢幕或按鈕等方式獲得同意時，應以相同簡易方式撤回同意
- 透過該服務特定使用者介面(例如網站登入帳號、app、IoT裝置介面)獲得同意時，應以相同介面撤回同意

第2016/679號規則(GDPR)中的同意之指引



本文摘取自國家發展委員會委託達文西個資暨高科技法律事務所執行之「GDPR相關指引文件研析」委託研究計畫結案報告，完整全文請至：https://www.ndc.gov.tw/News_Content.aspx?n=B7C121049B631A78&sms=FB990C08B596EA8A&s=97C7AD99A362EF7A。

ARTICLE 29 DATA PROTECTION WORKING PARTY
第29條個資保護工作小組

17/EN
WP259rev.01

Article29 Working Party
第29條個資保護工作小組

Guidelines on consent under Regulation 2016/679
關於第2016/679號規則(GDPR)中的同意之指引

Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018
2017年11月28日通過
2018年4月10日最後修訂並通過

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA
關於個人資料運用之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,
having regard to Articles 29 and 30 thereof,
having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日通過之95/46/EC指令而設立，
基於該指令第29條及第30條，
基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:
通過此份指引：

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.
由歐盟執委會司法總署C署（基本權利與歐盟公民）擔任秘書處，其地址為比利時，布魯塞爾B-1049，署MO-59 02/013號辦公室。

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936
網址：http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

趨勢九 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

開放銀行

Open Banking 早已有網路公司在做了

資料來源：https://moneybook.com.tw/

金管會三階段開放原則

第一階段
「公開資料查詢」：開放商品等公開資訊，以非交易面金融產品為主，如房貸利率、信用卡商品等，不涉及客戶資訊。

第二階段
「消費者資料查詢」：開放消費者資訊整合查詢，在客戶同意授權下，第三方公司提供帳戶整合服務。

第三階段
「交易面資訊」：開放交易資訊，第三方公司做帳戶整合後，可進一步透過App直接連結帳戶撥付，做消費支付，也可調整帳戶間資金。

→ 涉及個資法

資料法制框架

當事人同意
(15.0.2/19.1.5)

Open Banking

GDPR 資料可攜權

個人資料保護法

去識別化

匿名 vs 假名

企業
Open Data

政府資訊公開法

檔案法

政府
Open Data

Open Banking之法律誤解

議供參主管機關及業者參考。

1. 自願自律實屬短期做法，定期評估目前開放銀行相關機制運作狀況，視發展情況需要再採取修正措施

綜觀國際上對於開放銀行的運作架構，目前採取自願自律做法的國家(地區)除台灣之外，還有新加坡、香港、日本。由於目前採取強制開放的國家目前進展仍屬有限，建議我國可採取現行自願自律的發展政策，同時持續觀察後續發展情況。倘若未來定期評估時若發現我國在開放銀行發展進度上，確有落後於其他先進國家之情況，建議可盡快進行通盤檢討、修訂。

2. 開放銀行會員自律規範增定消費者同意開放資料之有效期限及後續資料處理方式，同時明確規定消費者可撤銷使用資料之授權

資料權最早源自於歐盟的法令規範，認為客戶對於自身的資料擁有權利，甚至對於議題應在未來資料保護相關法令明確界定，才能有助於銀行與第三方業者之間資料的流通使用。

參考歐盟 GDPR 作法，建議消費者每次同意的效期定為三個月，屆時需再經消費者同意才能再展延，並且每次徵求消費者同意開放資料的範圍、期限與最終處置都應說明清楚。為了確保第三方服務提供者獲取這些資料後，都用於原先設定的用途，因此要有「同意編碼(consent codification)」設計，也就是說依消費者同意的內容用途編碼，並加註到這些資料上，俾利日後追蹤這些資料的使用是否符合消費者開放的目的。

此外，根據 GDPR 第七條規定，消費者必須有改變主意的機會，並可撤銷之前同意的授權。但之前已經授權釋出給第三方服務公司的資料怎麼辦？消費者應該可依據 GDPR 第十七條被遺忘權規定，一旦撤銷其許可，之前開放的資料都應被刪除。所以，當消費者撤銷其同意，第三方服務提供者不但不能再取得新資料，已經蒐集的資料也應全部刪除。

GDPR無此規定

技術不可行

「同意之撤回」與「被遺忘權」無關

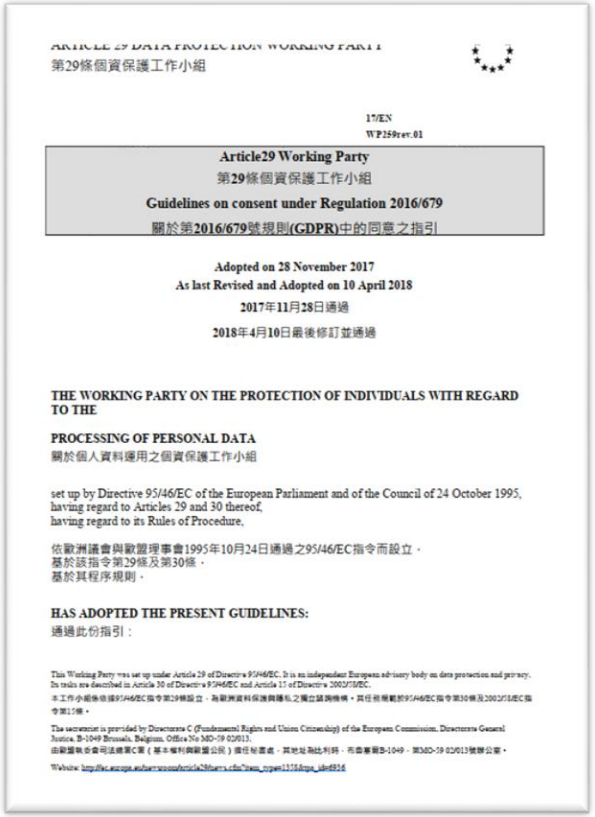
GDPR同意之指引

There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained.
GDPR對於同意的有效期限沒有特別限制。同意的效期應視個案背景、原始同意的範圍以及

30

當事人的期待而定。如運用作業有相當大的變更或演變，則原本的同意即不再有效。在此情形便須要獲得新的同意。

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights.[49]
WP29對最佳實務的建議是，同意應適時更新。再次提供全部資訊有助於確保當事人對於其資料如何被使用以及如何行使其權利，能保持良好的知情狀態[49]。



第29條個資保護工作小組

17/EN
WP259rev.01

Article29 Working Party
第29條個資保護工作小組
Guidelines on consent under Regulation 2016/679
關於第2016/679號規則(GDPR)中的同意之指引

Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018
2017年11月28日通過
2018年4月10日最後修訂並通過

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA
關於個人資料運用之個資保護工作小組

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,
having regard to Articles 29 and 30 thereof,
having regard to its Rules of Procedure,

依歐洲議會與歐盟理事會1995年10月24日通過之95/46/EC指令而設立，
基於該指令第29條及第30條，
基於其程序規則，

HAS ADOPTED THE PRESENT GUIDELINES:
通過此份指引：

資料來源：https://www.ndc.gov.tw/News_Content.aspx?n=B7C121049B631A78&sms=FB990C08B596EA8A&s=97C7AD99A362EF7A

Open Banking與PSD2

PSD2第4條第(17)、(18)、(19)點:

- 支付帳戶服務供應商（Account Servicing Payment Service Provider, ASPSP)
- 支付發動服務提供商（Payment Initiation Service Provider, PISP)
- 帳戶資訊服務提供商（Account Information Service Provider, AISP)

Fintech 發揮場域

Third-party Provider, TPP

歐盟推動Open Banking之法律基礎

PSD2第66條 (支付發動服務之支付帳戶存取規則)

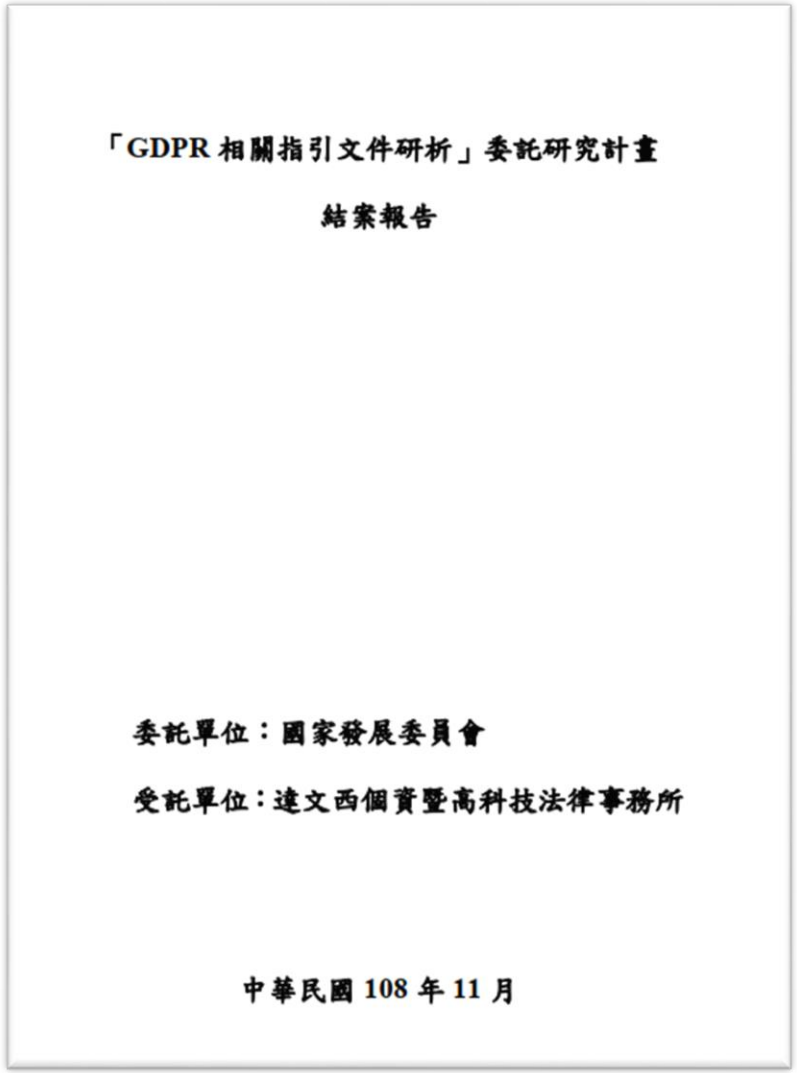
會員國應確保付款人有權利用PISP獲得支付發動服務，惟以支付帳戶可提供線上服務者為限。付款人按照第64條規定方式明確同意執行付款後，ASPSP應執行本條第4款規定的行動，以確保付款人使用支付發動服務之權利。

PSD2第67條 (帳戶資訊服務之支付帳戶資訊存取使用規則)

會員國應確保支付服務用戶有權利用AISP取得支付帳戶資訊，惟以支付帳戶可提供線上服務為限。

◆ **總結：** **PSD2明示允許在用戶明確同意及帳戶可提供線上服務之前提下，ASPSPs（銀行）須允許且配合合規之TPPs（Fintech業者）接觸客戶帳戶（Access to Account, XS2A）。**

延伸閱讀



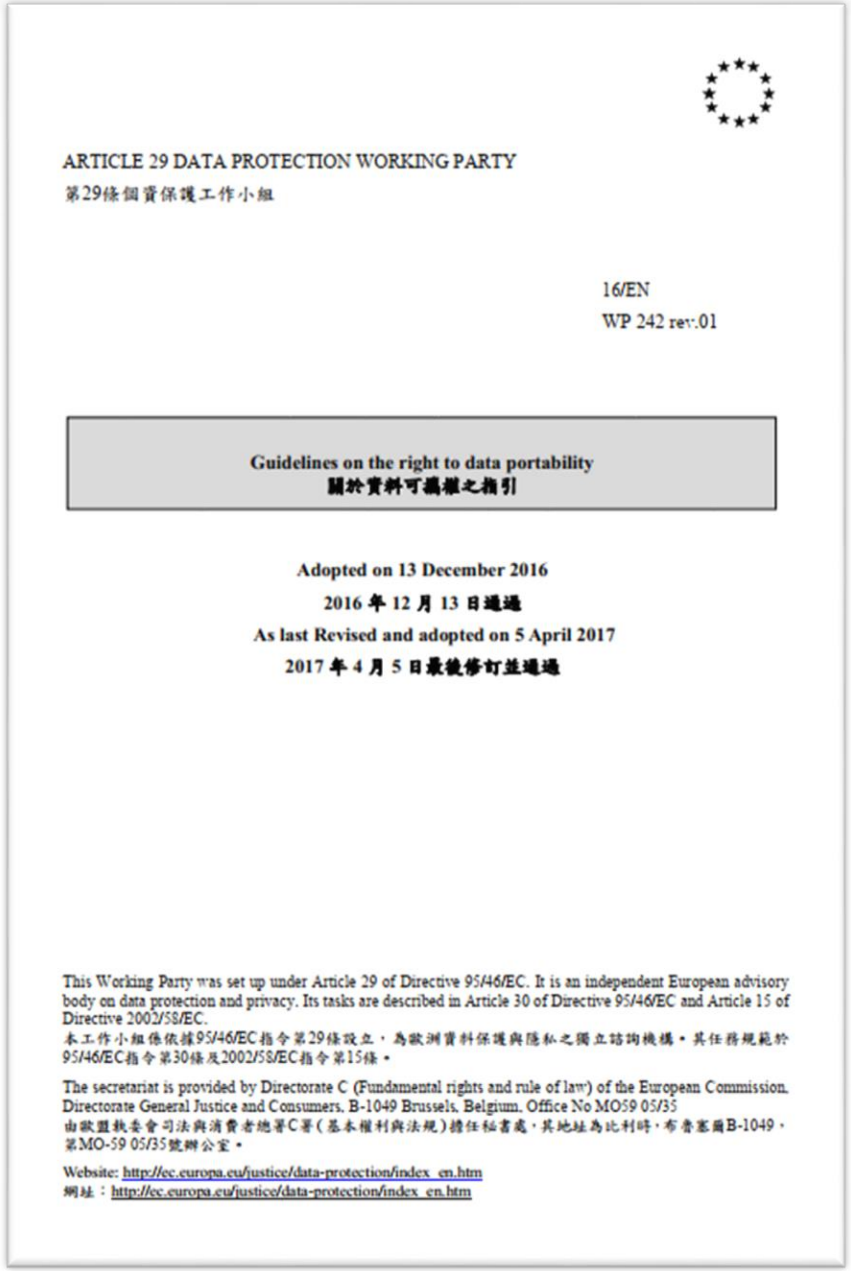
「GDPR 相關指引文件研析」委託研究計畫

結案報告

委託單位：國家發展委員會

受託單位：達文西個資暨高科技法律事務所

中華民國 108 年 11 月



ARTICLE 29 DATA PROTECTION WORKING PARTY

第29條個資保護工作小組

16/EN

WP 242 rev.01

Guidelines on the right to data portability

關於資料可攜權之指引

Adopted on 13 December 2016

2016 年 12 月 13 日通過

As last Revised and adopted on 5 April 2017

2017 年 4 月 5 日最後修訂並通過

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

本工作小組係依據95/46/EC指令第29條設立，為歐洲資料保護與隱私之獨立諮詢機構。其任務規範於95/46/EC指令第30條及2002/58/EC指令第15條。

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

由歐盟執委會司法與消費者總署C署（基本權利與法規）擔任秘書處，其地址為比利時，布魯塞爾B-1049，第MO-59 05/35號辦公室。

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

網址：http://ec.europa.eu/justice/data-protection/index_en.htm

資料來源：https://www.ndc.gov.tw/News_Content.aspx?n=B7C121049B631A78&sms=FB990C08B596EA8A&s=97C7AD99A362EF7A

中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範

遴選原則

- 由銀行對第三方服務提供者進行遴選，應注意檢視第三方服務提供者的背景、資格條件以及能力等。

要求遵循事項

- 銀行需要求第三方服務提供者遵循相關法規範，如有違反，銀行得終止雙方合作。

業務合作契約應訂定之事項

- 為維護銀行、消費者及第三方服務提供者之權益，銀行與第三方服務提供者之業務合作契約中應訂定下列事項，第三方服務提供者違反任一規定（包含權利義務、應遵循事項、智慧財產權歸屬及使用、消費者爭端解決機制、爭議處理機制、終止約定及事故通知），致損害消費者或銀行權益時，應負損害賠償責任，銀行並得終止合作契約。

開放銀行之思考

一、開放，源於資料自主原則

- 個資有所有權的觀念嗎?

二、GDPR資料可攜權

- GDPR中唯一具有競爭法性質之條文
- 促進個資自由流動

三、台灣個資法目前沒有資料可攜權→未來?

- 沒規定並不是不可做，但畢竟不是人民的權利

四、Open不限於銀行

- Open Banking是危機，也是轉機，更是商機

開放銀行之思考

五、數位轉型是因應Open潮流之關鍵

- 銀行應如何因應網路公司之挑戰?

六、TSP可否做到與銀行相同之資安水準?

- 木桶理論

七、一旦發生客戶資料外洩事件，賠償責任由誰負擔?

- 顧前主委：「就是找銀行負責，銀行先補償消費者，銀行再與TSP業者去釐清責任」

八、另需注意《金融機構作業委託他人處理內部作業制度及程序辦法》

- TSP適用委外辦法嗎?

九、台灣開放銀行適合用英國式強制開放或現行之自律開放?

趨勢十 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。

1942年 機器人三原則 艾西莫夫 (Isaac Asimov,1920-1992)

- 第一原則是機器人不得傷害人類，或看到人類受到傷害而袖手旁觀；
- 第二原則是機器人必須服從人類的命令，除非這條命令與第一條相矛盾；
- 第三原則是機器人必須保護自己，除非這種保護與以上兩條相矛盾。

2016年 微軟CEO Satya Nadella 提出AI六原則

- AI 必須用來輔助人類
- AI 必須是透明的
- AI 必須實現效能最大化，同時又不能傷害人的尊嚴
- AI 必須用於智慧隱私
- AI 必須承擔算法責任以便人類可以撤銷非故意的傷害
- AI 必須防止偏見

2019年 歐盟人工智慧七大道德準則

- AI 不應侵犯人類自主性與自由
- AI 應具資訊安全性與正確性
- AI 蒐集的數據得受到安全且隱密的管理
- 建構 AI 的系統與演算法得公開且得以追溯到開發者
- AI 需具備多元性與公平性，不行以年齡、性別、種族作為分類標準
- AI 需促進社會正面改變，且具備永續性（例如，AI 應保持環保的概念）
- AI 需建立咎責機制

AI道德規範是規範人類？還是規範AI？

- 人類不應侵犯人類自主性與自由
- 人類應具資訊安全性與正確性
- 人類蒐集的數據得受到安全且隱密的管理
- 建構人類的系統與演算法得公開且得以追溯到開發者
- 人類需具備多元性與公平性，不行以年齡、性別、種族作為分類標準
- 人類需促進社會正面改變，且具備永續性（例如，人類應保持環保的概念）
- 人類需建立咎責機制

◆ **道德規範是否足夠？未來是否有必要針對AI立法？**

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